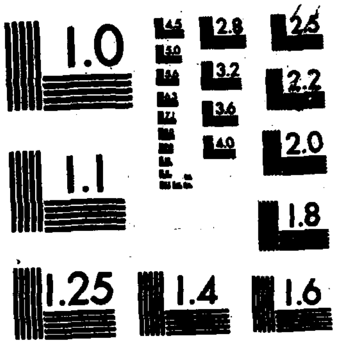
AD-A126 768 COMPUTER SECURITY FOR THE COMPUTER SYSTEMS MANAGER(U) 1/1
NAVAL POSTGRADUATE SCHOOL MONTEREY CA W D HELLING
DEC 82

UNCLASSIFIED F/G 9/2 NL

END


1.0
4.5
5.0
5.6
6.3
7.1
8.0
2.8
3.2
3.6
4.0
2.5
2.2
2.0
1.1
1.8
1.25
1.4
1.6

2

NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

COMPUTER SECURITY FOR THE
COMPUTER SYSTEMS MANAGER

by

William D. Helling
December 1982

Thesis Advisor: Norman Lyons

Approved for Public Release; Distribution Unlimited

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

REPORT DOCUMENTATION PAGE		READ INSTRUCTIONS BEFORE COMPLETING FORM
1. REPORT NUMBER	2. GOVT ACCESSION NO. A126768	3. RECIPIENT'S CATALOG NUMBER
4. TITLE (and Subtitle) Computer Security for the Computer Systems Manager		5. TYPE OF REPORT & PERIOD COVERED Master's Thesis December 1982
		6. PERFORMING ORG. REPORT NUMBER
7. AUTHOR(s) William D. Helling		8. CONTRACT OR GRANT NUMBER(s)
9. PERFORMING ORGANIZATION NAME AND ADDRESS Naval Postgraduate School Monterey, California 93940		10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS
11. CONTROLLING OFFICE NAME AND ADDRESS Naval Postgraduate School Monterey, California 93940		12. REPORT DATE December 1982
		13. NUMBER OF PAGES 81
14. MONITORING AGENCY NAME & ADDRESS(if different from Controlling Office)		15. SECURITY CLASS. (of this report)
		15a. DECLASSIFICATION/DOWNGRADING SCHEDULE

16. DISTRIBUTION STATEMENT (of this Report)

Approved for Public Release; Distribution Unlimited

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

18. SUPPLEMENTARY NOTES

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)

Computer Security, Security Kernel, Risk Management, Computer Threats, Countermeasures

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)

This thesis is a primer on the subject of computer security. It is written for the use of computer systems managers and addresses basic concepts of computer security and risk analysis. An example of the techniques employed by a typical military data processing center is included in the form of the written results of an actual on-site survey. Computer security is defined in the contect of its scope and an analysis is made of those laws and regulations which direct the application of security measures into Automatic(Continued)

Abstract (Continued) Block 20

Data Processing Systems. Finally, a list of some of the major threats to computer security and the countermeasures typically employed to combat those threats is presented.

Approved for public release; distribution unlimited.

Computer Security
for the
Computer Systems Manager

by

William D. Helling
Major, United States Marine Corps
B.S., University of West Florida, 1977

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION SYSTEMS

from the

NAVAL POSTGRADUATE SCHOOL
December 1982

Author: W. D. Helling

Approved by: Norman R Lyons
Thesis Advisor

William R. Shockley
Second Reader

Chairman, Department of Administrative Sciences

W M Woods
Dean of Information and Policy Sciences

ABSTRACT

This thesis is a primer on the subject of computer security. It is written for the use of computer systems managers and addresses basic concepts of computer security and risk analysis. An example of the techniques employed by a typical military data processing center is incluied in the form of the written results of an actual on-site survey. Computer security is defined in the context of its scope and an analysis is made of those laws and regulations which direct the application of security measures into Automatic Data Processing systems. Finally, a list of some of the major threats to computer security and the countermeasures typically employed to combat those threats is presented.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

I. INTRODUCTION

A. BACKGROUND

During the last fifteen years, the use of computers and other automatic data processing equipment has increased at an exponential rate and many computer industry analysts predict that the proliferation of computer applications will continue into the next century. To keep pace with the demand for better and faster systems, the computer industry has responded with advances in hardware and software technology, system design methodology, improved management philosophies and similar improvements in almost all other computer-related disciplines. One area that has lagged behind the technology avalanche is that of computer security. The annual loss of perhaps millions of dollars through deliberate and covert penetrations of computer-based information systems as reported by Allen and as partially listed in Table I is merely the tip of the iceberg. There are many companies that withhold acknowledgements of successful penetrations of their systems and many who are not aware that their systems have been penetrated. There are penetrations that compromise classified information and penetrations that cause personal loss through the violation of privacy. If one were to put a true monetary value on all the losses mentioned here, Allen's estimate of millions of dollars lost would be pale by comparison. The severity of the computer security problem and the gigantic financial and personal losses that it involves might lead one to believe that the computer industry, the federal government, or the academic community would have long ago discovered a remedy. While it would not be realistic to expect a method for

TABLE I

A Survey of Computer Frauds

SUMMARY	AMOUNT
1. Clerk at storage facility entered information into computerized inventory system to mask theft of inventory. Shipments made without billing.	$ 4,000,000
2. Warehouse employees manipulated computerized inventory system through unauthorized terminal entries to mask inventory thefts.	$ 200,000
3. Officer of London bank stole funds from inactive accounts.	$ 290,000
4. Bank employee misused on-line banking system to perpetrate lapping fraud including unrecorded transactions, altered transactions, and unauthorized account transfers.	$ 1,400,000
5. Manufacturing company manager who had designed and installed automated accounting system used it to steal.	$ 1,000,000
6. Organized crime ring operated check-kiting fraud between two banks using computer room employees who altered deposit memos to record check deposits as available for immediate withdrawal.	$ 900,000
7. Accountant at large wholesaler established phony vendors through computerized accounting system that he operated.	$ 1,000,000
8. Officer of brokerage house misappropriated company funds through computer system that he controlled.	$ 277,000
9. Director of publishing subsidiary manipulated computer system to add false sales and block recording of accounts payable - all to improve operating results, thereby securing a position on the board of directors.	$11,500,000
10. Clerk in department store established phony purchases and vouchers paid to a friends company.	$ 120,000
11. Customer representatives of large public utility, together with outside associate, erased customer receivables using customer error correcting codes; received kickback from customer.	$ 25,000

[Ref. 1: p. 61]

guaranteeing a one-hundred percent secure system, it is reasonable to expect that a computer based information system could be constructed that would at least prevent most of the penetrations. The truth is that the technology and the procedures are available and they would be effective if computer systems managers would only use them. The reasons for not using computer security measures will be covered later. Suffice it to say at this point that managers are finally waking up to the fact that computer security is something to be concerned about.

The current and increasing concern for data security is the result of three major interrelated factors.

The first is the dramatic technological advancement in automatic data processing equipment and software systems mentioned briefly above. In a modern computer environment, multiple jobs and/or multiple users can concurrently access the facilities and the stored data of the system. Computation speeds are fast approaching billions of operations per second, and the amount of stored data ranges well into the billions of bytes. Each of a variety of users has a variable security authorization and the data sets themselves have diverse security requirements.

The second factor is the increasing need of science, industry and government for processing vast quantities of data as quickly as possible. Further, decreasing per-unit processing and storage costs have increased the number of applications economically feasible to automate.

The third factor, the result of greater availability of communications facilities and terminal devices, is the increasing emphasis on providing computer access at remote operations levels. Much effort in recent years has been devoted to simplifying the interface between the user and the computer. As a result, many systems provide guidance and computer- assisted instructions to help the user become increasingly productive and increasingly knowledgeable.

These developments have led to systems that permit the users to do their jobs faster and better. As the access to information is extended, however, so must the security measures that control this access. The computer systems manager faces increasingly difficult decisions as a result of this information extension. The decisions stem from the need to balance the risk of the loss threatened with the cost of countermeasusres. Risk management, as this balancing process is called, is an imprecise science and is a relatively new field of study for the computer professional. As such, the subjective assessments and judgements of the manager must be inordinately relied upon throughout the process. The scope of the security problem approaches infinity and the term "secure" must be considered, at best, a temporary state of any system. The budget constraints of many organizations, both public and private, tend to limit the programs and projects that managers can pursue. If those organizations have never experienced security problems, the opposition by upper level management to the application of security measures can be anticipated. One final aspect of computer security can complicate the manager's task. Even if the conscious decision by all levels of management is made to install secuity safeguards, the task of retro-fitting an unsecure system is not easy. The process of "designing in" security is much more preferable and the historical efforts to "bolt on" security have been expensive and largely unsuccessful due to a lack of sophisticated analysis.

The computer systems manager, and more explicitly, the security manager must possess a myriad of skills and abilities, foremost of which is the ability to produce cost effective techniques for maintaining or raising the security level of his system without significantly increasing the complexity of the user interface. He must also be capable of constant vigilence for as soon as he relaxes, the advantage goes to the potential penetrator.

Good security is not a conglomeration of individual countermeasures fending off specific secuity threats. it is a well designed system of countermeasures that act in unison to protect the whole system. Risk management is the process by which this design is constructed and implemented.

B. OBJECTIVES

Many formal education programs are geared explicitly to the prospective computer systems manager. While these programs provide the would-be manager with the general skills required of the occupation, most of them only briefly address computer security and then only as an ancillary topic. The objective of this thesis is to supplement formal computer systems education by providing the junior computer systems manager with a non-technical, conversational knowledge of computer security. Toward this end, a moderately concise definition of the subject is presented along with an assessment of the subject scope. Additionally, a brief overview and analysis of the laws and regulations pertaining to computer security is presented. This is followed by a discussion of risk management and some of the techniques it employs. An enumeration of the chief threats to computer security and the countermeasures typically employed to combat those threats follows and finally, the results of a computer security survey of an actual military data processing center is offered as an exercise in security assessment and as an indicator of how computer security is addressed in the real world.

II. COMPUTER SECURITY DEFINED

Most literature dealing with the subject of computer security attempts, at some point, to define the term. A fault with many of these definitions is that they are presented in abstract, and therefore, not very useful terms. Others, although adequately defining computer security in useful terms, fail to describe its scope. Since the scope of the term is surprisingly broad, a good working definition should include at least an overview of the topic. One of the few useful definitions of computer security encountered in the literature survey for this thesis comes from Pritchard [Ref. 2: p. 7]. In his book, Pritchard describes general classifications of losses due to breaches in computer security. These classifications are:

A. Loss of system availability

B. Loss of system integity

C. Loss of system confidentiality

In order to fully appreciate a computer security definition, it is useful to be acquainted with the scope of the subject. Although the subject of risk analysis will be treated in later chapters, in order to adequately describe the scope of computer security, it is useful to present a overview analysis of threat classifications at this point in order to give the reader some indication of the size of the problem. Using Prichard's loss classifications, general threat categories are listed below:

A. LOSS OF SYSTEM AVAILABILITY

There are many ways that system availability can be affected. Depending on the size and the distributed nature of any particular system, the general assets of that system include seven basic categories. The general vulnerabilities of each asset category are listed in the following sections.

1. Hardware

The hardware of any system is the foundation upon which all other components of a computerized information system rest. When hardware assets are lost, system performance decreases - sometimes to zero. Some general vulnerabilities of hardware are:

- support dependency
- physical attack
- design reliability
- natural catastrophe
- operator dependency

2. Software

Software is the collection of instructions that directs the hardware through its required operations. As software assets are lost, some measure of performance is also lost. Some general software vulnerabilities related to system availability are:

- susceptibility to modification
- wide accessibility
- ability to hide subversion techniques
- design reliability

3. Data and Documentation

These two computer system assets are grouped together because they are closely related in that they are both vulnerable to similar threats. Data is the resource upon which the hardware/software combination operates. Documentation is the set of operating instructions. Loss or degradation of either or both of these assets renders a system useless or counterproductive. Some general documentation and data vulnerabilities are:

- modification susceptibility
- destruction susceptibility

4. Communications

The communications aspects of a given system can be as complicated as a multi-noded distributed system linked by microwave and satellite relay or as simple as a quarter inch cable leading to off-line storage in the next room. Partial or complete loss of communications between system nodes or components can result in a spectrum of problems ranging from complete system collapse, to the failure of a particular applications package. Some vulnerabilities of communications assets are:

- subceptability to interception
- subceptability to jamming or blocking
- hardware/software dependent

5. Environment

Although the reliability of computer hardware has increased in recent years, the technological precision of many hardware components has also increased thereby making environmental assets such as air conditioning, humidity control, and power sources essential to system availability. Environmental degradation can cause system collapse or simply make the area uncomfortable work in. Environmental weak points are:

- design reliability
- support dependency
- adaquacy
- operator dependency

6. Support

Support is the word that describes all those activities not part of the information processing system itself, but without which the system could not function. Examples of support activities range from the steaiy, uninterrupted delivery of continuous form paper to the steady, uninterrupted delivery of electrical power. Interruption of support can disrupt an information system by varying degrees and the effects of such a disruption depends upon the effectiveness of contingency planning.

B. LOSS OF SYSTEM INTEGRITY

The most common application of the term "system integrity" is to the data on which a system operates. A useful definition of data integrity is

> the state existing when data agrees with the source from which it is derived, and when it has not been either accidentally or maliciously altered, disclosed, or destroyed [Ref. 3: p. 7].

This aspect of computer security is perhaps the most difficult to guard against because it is usually the most difficult to detect. An inadvertant or malicious degradation in data integity can have varying results ranging from the taking of action based on incorrect information to the crash of the entire system. In most cases, the discovery of the lack of data integrity is after the fact. Some generic types of data integrity vulnerabilities are:

- accidental or malicious entry errors
- accidental or malicious processing alterations

C. LOSS OF CONFIDENTIALITY

Loss of confidentiality probably describes the thought that comes immediately to mind whenever the topic of computer security is mentioned. It is potentially the most serious result of an insecure system. Federal Information Processing Standards (FIPS) #41 defines confidentiality as

> a concept which applies to data. It is the status accorded to data which requires protection from unauthorized disclosure.

This definition, although useful, is perhaps a bit narrow. Substituting the word "information" for the word "data" in the definition broadens the definition appreciably and points to an important theoretical concept. Information is the result of data processing or manipulation. Data itself is analogous to the words in a dictionary. Each word contains a value or meaning but when combined with other words in a process called language, the sum of the words conveys a concept or idea. Data is merely the conglomeration of unassociated fields (words). The problem of data security therefore, transends the collection of data fields and extends to the process through which those fields are processed into information. In this thesis, the treatment of the security problem is restricted to data and its processing, but the reader should be aware that information security is a much larger concept that only begins at the point of processing. The losses suffered from a lack of confidentiality are usually evaluated first in a typical risk management scenario because those safeguards put in place to protect system confidentiality many times solve problems in the other loss categories. Some general threats to confidentiality are:

- accidental or intentional interception
- unauthorized access

D. DEFINITION

The above discussion of loss categories and their subsets is presented to impress the reader with the scope of the computer secuity problem. With the immense proportions of that problem in mind, the following definition of computer secuity is offered:

> Computer security is the protection of computing assets or resources and computer based systems against accidental and deliberate threats whose occurrance may cause losses due to those systems' non-availability, lack of integrity, or lack of confidentiality.
>
> [Ref. 2: p. 7]

III. AN ANALYSIS OF SECURITY LAWS AND REGULATIONS

The need for computer security was not of primary concern to computer systems managers during the accelerated growth of the computer industry in the 1970's. Managers of information systems were much too busy dealing with great technological leaps in the hardware and software offerings of major vendors. The efforts to maintain security were largely ineffective because of the lack of management support and because of the predominantly after-the-fact design of security safeguards - the "bolt on" security systems mentioned earlier. Due to articles such as that of Allen [Ref. 1: pp.52-62] and Moffett [Ref. 4: pp. 124-126] and other preceding authors, the public soon became aware of the potential and actual misuse of data and information systems. Articles concerning the misadventures of unsuspecting citzens and their battles with credit agencies, banks, and billing and collecting firms were not uncommon in the media. Finally, due to public pressure on legislators for protection against the invasion of privacy and for a legal method of correcting incorrect or incomplete personal data, two major laws were ratified by the Congress. This legislation had the ultimate effect of making computer systems managers more aware of the need for data privacy and data integrity. The history behind other laws, regulations, and directives is not quite as colorful, but the fact that they exist in large quantities is, no doubt, a commentary on the vulnerability of computer files and data to mistreatment, broad access, and disclosure. The following sections of this chapter contain a brief analysis of the regulations and laws that affect the computer systems managers of the federal government. The discussion is arranged in two categories. The first category deals with regulations affecting organizations within the federal government; the second category is a generalized treatment of agency-specific directives.

A. THE PRIVACY ACT AND OTHER LEGISLATION

1. The Privacy Act of 1974

The Privacy Act of 1974 imposes numerous requirements upon federal agencies to prevent the misuse or compromise of data containing personal information. Federal automatic data processing (ADP) organizations which process personal data must provide a reasonable degree of protection against unauthorized disclosure, destruction, or modification of personal data, whether intentionally caused or resulting from accident or carelessness. These requirements demand the application of managerial, administrative, and technical procedures. FIPS #41 addresses the requirements and the corresponding safeguards used to implement the provisions of the Act. Table II lists those items.

Two desirable by-products of the Privacy Act are the promotion of risk analysis and the elimination of unnecessary data, a procedure undertaken to narrow the range of the safeguards used. Both of these side effects aided in the development of more secure systems; the risk management promotion in refining the techniques of a little used procedure, and the purging of files in creating more concise, manageable data bases.

2. The Freedom of Information Act

The Freedom of Information Act requires federal agencies to publish in the Federal Register, certain information related to personal files. This information must include the source and method by which the information

TABLE II

Privacy Act Requirements and Safeguards

REQUIREMENTS	SAFEGUARDS
Control of Disclosures	Entry Controls
Accounting of Disclosures	Storage Protection
Access to Records	Data Handling
Disputed Information Inclusion	Record Maintenance
Use of Relevant Data for Authorized Purposes	Data Processing Practices
Accurate, Complete Records	Responsibility Assignment
Insurance of Integrity, Security and Confidentiality	Auditing
Record Retention	Data Encryption
	Identification

[Ref. 3: p. 8]

retained by those agencies can be obtained. Additionally, the Act requires that a general discription of the data, the processes that act upon the data, and the results of those processes be available through the channels described in the Federal Register. The Act appears to be loosely worded and has many exceptions thereby diluting some of its effectiveness. Once again, however, the awareness level of federal agency information system managers to computer security was raised. The Act compels the manager to establish, at least, a defensible security policy and a set of corresponding procedures for the prctection of data.

3. Office of Management and Budget (OMB) Circular A-108

OMB Circular A-108 is the implementation of the Privacy Act of 1974. It, along with the guidelies of FIPS #41, put teeth into the Privacy Act by explaining, point by point and in specific terms, the administrative procedures to be followed and the policies to be established by all federal agencies. Although computer files are not addressed in A-108, and therefore no technical procedures for protecting computer files, the underlying effect of the circular is to reinforce top management's support of data security.

4. Code of Federal Regulations, Part 6 of Title 15

This regulation deals with the standardization of data elements and representations. Although only peripherially associated with security, it is included here for two reasons. First, it illustrates the initial efforts of the federal government to establish a huge distributed system of data bases that could extend the capability of agency-to-agency data exchange. Secondly, while the concept of of standardization is a sound managerial technique for promoting efficiency, it simplifies the potential penetrator's task by not only aiding the standardization of his efforts, but also, increasing the number of potential entry points where he might access the information.

B. AGENCY SPECIFIC REGULATIONS AND DIRECTIVES

Most of the material in this category belongs to one of two sub-categories.

The first subset includes agency procedures for handling classified information. Usually, only brief mention of classified computer files is made in this type directive. Some physical security procedures are directed but no technical information is included.

The range of specific security aspects covered in these directives is generally good, but directions as to the technical implementation of policies within a specific facility is not. The absence of technical procedures facilitates the diversity of hardware and software throughout the agency. It also allows subjective judgements to be made at the installation level as to threat assessment and appropriate safeguards. The potential exists, at the installation level, for the subjective judgements of management personnel to be influenced by the operational workload, the manning level, and the technology level of the installation hardware and software. That being the case, the strengths of individual programs may vary significantly. Examples of such directives are contained in DODD 5200.28, OPNAV 5239.1 (Navy), and MCO P5510.14 (Marine Corps).

The second category of agency specific directives are locally developed security plans applicable only to the individual activity. These documents should be, and for the most part are, the embodiment of all higher directives and tailored to the local environment. Again, considerable flexibility is allowed. Security plans offer a wide variance in coverage. What is more, the enforcement of local security plans also varies widely.

IV. RISK MANAGEMENT

A. OVERVIEW

Computer security is initially concerned with determining and implementing cost-effective countermeasures to make a system secure against the many threats which can occur. It is concerned, therefore, with reducing the frequency with which any threat is expected to occur and/or reducing the impact of the threats upon the correct functioning of the system. Secondly, it is concerned with what has to be done when the normal mode of operation is disrupted. It is concerned with contingency planning, that is, the preparation and execution of a standby mode of operation and with the preparation and execution of recovery plans. The third concern of computer security is the auditing of the system in both the normal and standby modes of operation [Ref. 2: p. 2].

Risk management is the name given to the process by which all three of the above concerns are dealt with and its objective is to protect the system from losses resulting from these concerns. Its organization is variable, that is, task organized to the specific need, but the major methodologies employed are basic. They are

- threat identification
- threat impact measurement
- countermeasure identification and measurement
- countermeasure selection
- implementation and monitoring of safeguard effect

There are several good references on the topic of risk management (see bibliography) and since this thesis deals with the subject as a subset of computer security, only a cursory look will be taken at some of the procedures it employs.

Risk management is essentially concerned with developing and maintaining a cost-effective security program. The optimal point at which the employing organization should operate is as illustrated in Figure 4.1 The downward sloping curve (curve A) illustrates the effect on losses as countermeasures are applied. The upward sloping curve (curve B) is the cost of the countermeasures as they are successively applied. The U-shaped curve (curve C) above the intersecting lines is the total of both the cost of losses and the cost of countermeasures. The optimum operating position is, quite obviously, the lowest point (point O) on the U-shaped, or total cost, curve. The distance between the X-axis and the low point on the total cost curve is the total number of dollars spent on countermeasures plus the total number of dollars lost due to security breaches when operating at the the optimal level. The total number of dollars is read on the y-axis at the point (point P) horizontal to and left of the low point. The level of protection is represented by the length of line (E) and read on the x-axis at point (Q). The total number of dollars expended in either of the two ways is affected, of course, by the effectiveness of the countermeasures employed. One of the most effective countermeasures is the reduction of the number of personnel authorized access and the reduction of the number of access points. Successive reductions in either the authorized personnel or the access points certainly will solve the security problem, but it also reduces the availability of information to the organization which, in turn, decreases the organization's ability to function properly. This also causes a loss. Some

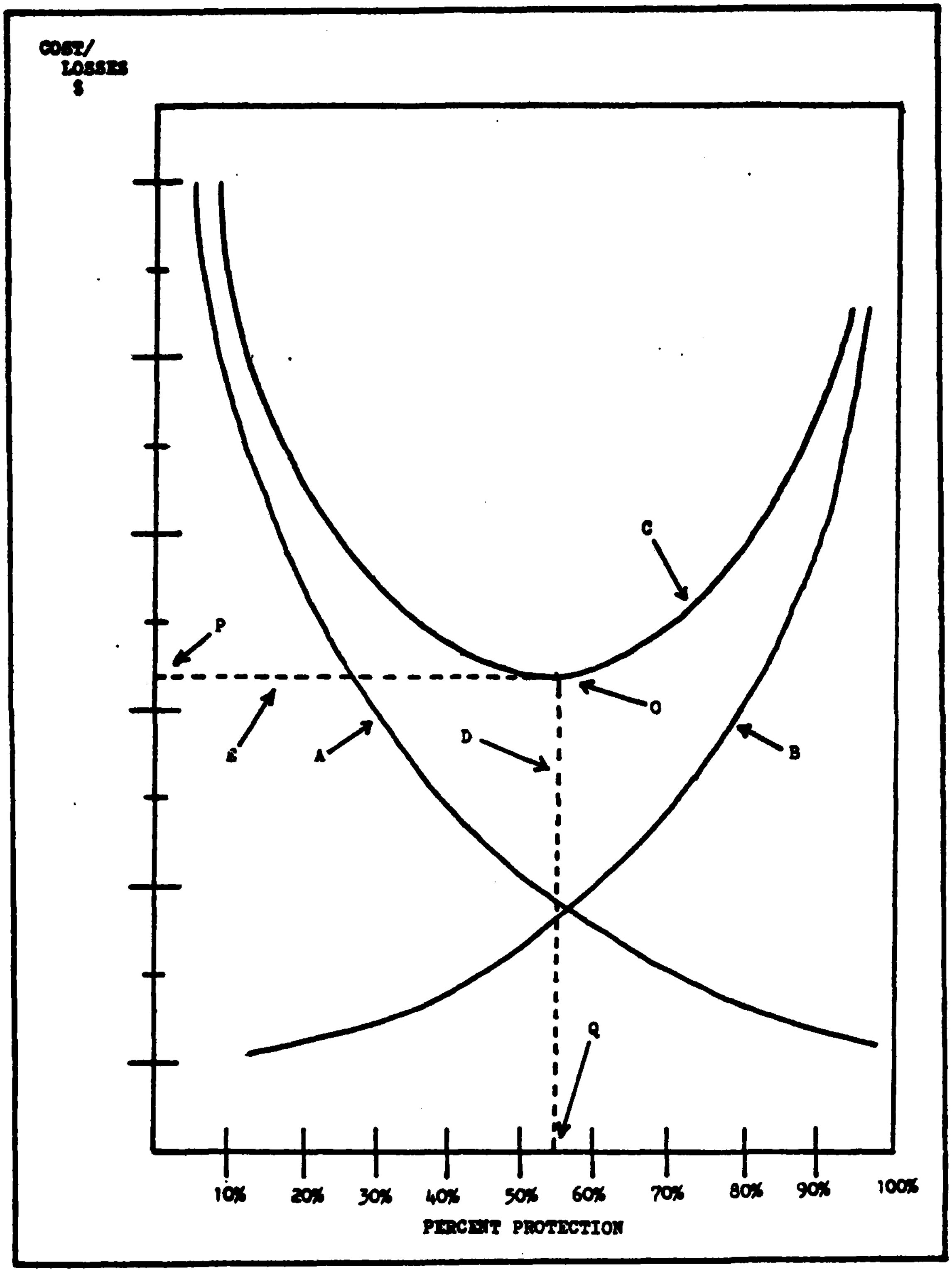


Figure 4.1 The Optimal Level of Computer Security.

middle ground must be found and that is point (O) in the figure. The underlying point to all this is that it is the risk manager's job to reduce the threat of security in the most cost effective way while maintaining the level of information availability. Some other interesting points are illustrated in Figure 4.1 . Note that the total cost curve (C) appears to approach the vertical asymtotically on the right. The futher projection of this line might reveal that it, in fact, doubles back to the left at some point. This graphically represents the fact that at some point, far to the right of the optimal operating point, the successive application of countermeasure upon countermeasure will become counterproductive. Note also that the curve representing countermeasure expenditures (B) never quite reaches the one hundred per cent protection vertical from the x-axis. Another point to note is that there remains a vertical distance between the x-axis and the loss curve. This says that the losses are never cut to zero.

Although risk management involves the countering of secuity threats in three aspects, only cost-effectiveness determination will be discussed in this chapter. The aspects of contingency planning and auditing will be treated in Chapter six.

B. COST EFFECTIVENESS DETERMINATION

As discussed before, the third part of risk analysis is the analysis and application of cost effective countermeasures. This process has essentially three distinct steps (threat assessment, countermeasure assessment, countermeasure selection) which are discussed below.

1. Threat Assessment

Threat assessment is composed of three components. The first component is the identification of the threats applicable to the system in question. The list of threats will certainly be different for each individual system but they are all determined in a, more or less, subjective manner. Decomposing threats into threat categories is the first step. A manager may wish to use a decomposition similar to that of Figure 4.2 or he may use a checklist such as was used to determine the threat categories in Chapter 7. In either case, the final decomposition of the threat is usually done by the checklist method. Marine Corps Order P5510.14 and OPNAVINST 5239.1 contain examples of checklists.

The second component of threat assessment is the determination of threat occurrence frequency. This information can be obtained through the use of the organization's historical data or can be derived from the study of other similar organizations. Much effort should be expended to determine frequency as accurately as possible for it will figure significantly into the cost computations of countermeasures as will be demonstrated later in the process.

The next, and final, step in threat assessment is the determination of total exposure. This procedure is no more than the multiplication of the factors determined in the first two components using the following formula:

$$T = N1 \times C1 + N2 \times C2 + \ldots\ldots. + Nn \times Cn$$

where T is the total loss (usually expressed in terms of dollars) per year. It is the expected annual loss from all threats combined. Nn is the total number of occurrences of a single threat expected annually and Cn is the amount of loss per occurrence. The product of each threat and it's frequency is added to the product of all other threats and frequencies thereby yielding T.

2. Countermeasure Assessment

The second component of cost effectiveness determination is the assessment of countermeasures. At this point, a slight digression is in order. Countermeasure accessment involves the evaluation of the effectiveness of various countermeasures and as such can become very complicated as the number of the countermeasures under analysis increases. The task of the manager can be simplified somewhat by classifying countermeasures by the method used to handle threats. Four general methods for handling threats are commonly used. The first is threat avoidance. Threat avoidance involves isolating the component(s) vulnerable to the threat and eliminating those component(s). Since most system components are vulnerable to some sort of threat, if this method were used exclusively, it would be only a matter of time until there was no system. The second method of threat handling is threat retention. Threat retention is usually employed when T = Nn X Cn is small for a particular threat. A threat in this category is either ignored or handled in conjunction with the third threat handling procedure - threat transfer. Threat transfer is nothing more than the utilization of some sort of insurance to offset the effects of the threat. Threat reduction, the fourth threat handling procedure, is, by far, the most common. It is the application of positve steps or devices designed to reduce the number of threat occurrences and the effects of each threat. Some examples are physical access control, processing restrictions, and tempest shielding.

The next step in countermeasure assessment is the determination of effectiveness. For example, if countermeasure XYZ reduces the frequency (N) of a threat from ten incidents to one incident per year; and the loss per incident from $1,000 tc $850, the effectiveness of the countermeasure can be given a numerical quantification as follows:

$Nn' X Cn' = T'$

(Total loss per occurance with countermeasure)

then

T' = $850 utilizing countermeasure XYZ

T = $10,000 without countermeasure XYZ

therefore

$(T - T') / T =$ effectiveness

substituting

($10,000 - $850) / $10,000 = 0.915

This says that countermeasure XYZ is 91.5% effective.

3. Countermeasure Selection

One method of countermeasure selection is presented below by the continuation of the example above.

Suppose countermeasure XYZ costs $5,000 to implement and has a failure rate of 8.5% (100% - 91.5%). The total cost of using the measure is computed as follows:

$Tc = T + Cf - T(1 - P)$

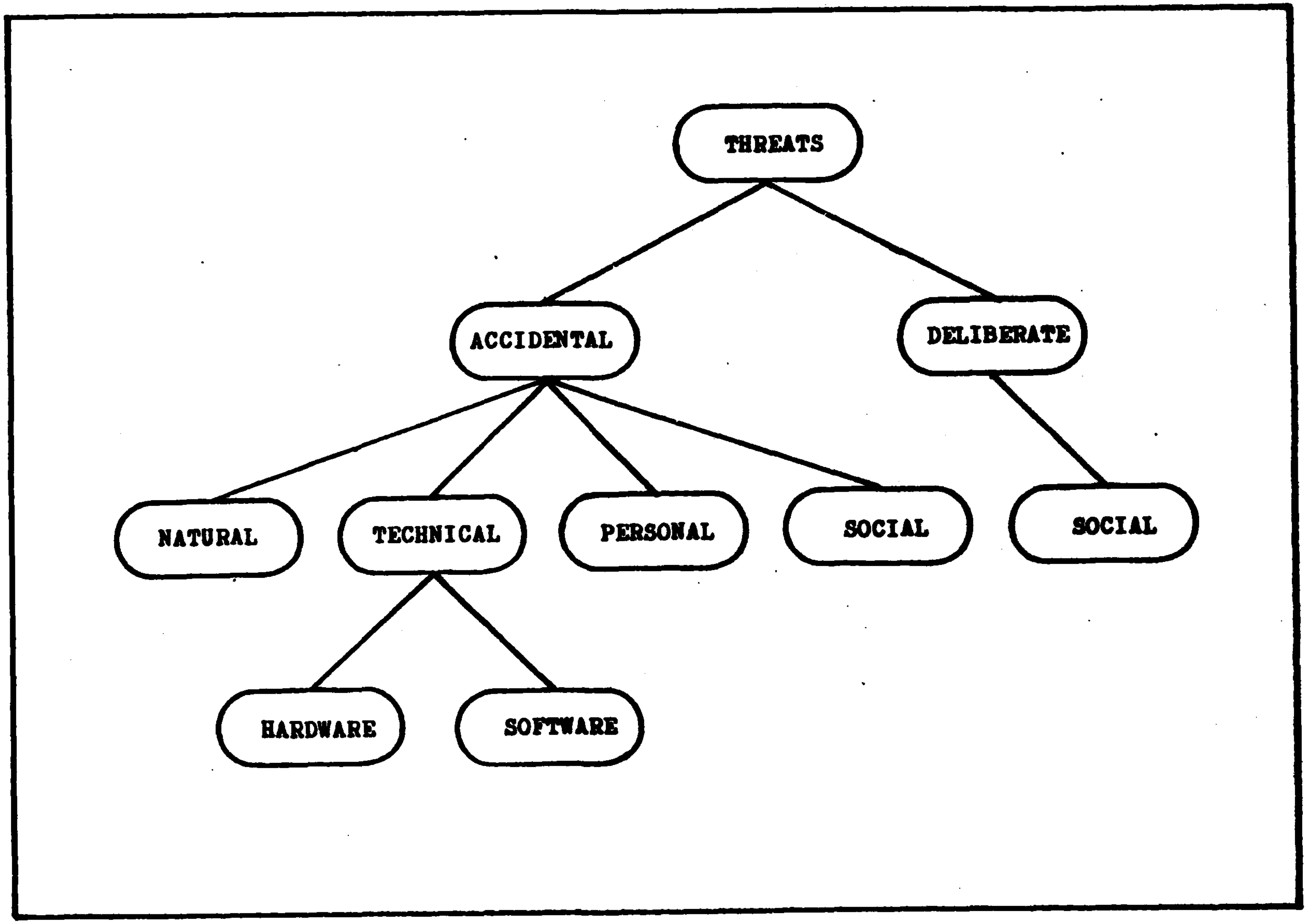


Figure 4.2   Decomposition of the Threat.

where

Tc = total cost
T = Nn X Cn (as computed above)
Cf = cost of implementation

for our example

T = $10,000
Cf = $5,000
P = .085

and

$$\begin{aligned} Tc &= \$10,000 + \$5,000 - \$10,000(1 - .085) \\ &= \$10,000 + \$5,000 - \$9,150 \\ &= \$5,850 \end{aligned}$$

This final figure is the total loss to the using organization. Total losses of $10,000 were sustained prior to countermeasure XYZ employment. After countermeasure XYZ employment, total losses where $5,850 ($5,000 of which were implementation expenses). The countermeasure, then saves $4,150 ($10,000 - $5,850) the first year, and $9,150 ($10,000 - 850) in each succeeding year.

The simple example above was derived from the procedures shown in FIPS #31 [Ref. 5: pp. 12-13]. Note that the procedure involves the use of only one countermeasure. Not only are several measures compared, in most cases, but discounting techniques are also used. This is but one method of determining cost effective countermeasures. Other equally valid and effective techniques are mentioned in bibliographical references.

V. THREAT ANALYSIS

The scope of computer security, as discussed in chapter 2, approaches infinity. The topic's large size is a direct result of the large number of potential threats to the computer system. Since any discussion of computer security threats must be finite, that discussion must, therefore, be incomplete. With that in mind, this chapter will seek to present both general and specific threats to computer security along with some of their effects.

Pritchard [Ref. 2: p. 19] and Carullo and Shelton [Ref. 6: p. 52] describe various methods for decomposing threats into classifications. One such classification is illustrated in Figure 5.1 reprinted here for convenience. Note that this example could be modified by the addition of "Hardware", "Software", and "Personal" under "Deliberate - Social". Checklists are another way of identifying threats. Checklists usually reflect the needs of their composers and a specific computer system and, therefore, are not usually complete. A checklist composed of several checklists from different sources may prove to be fairly comprehensive. This is essentially the technique used in the construction of the following list. Four main references [Ref. 5: pp. 77-82], [Ref. 7: pp. 3.3-9.15], [Ref. 8], and [Ref. 9: pp. G1-G50] were used. For the purposes of this thesis, threats are organized into the following categories:

- physical threats
- emanations
- hardware threats
- software threats
- personnel threats
- procedural threats

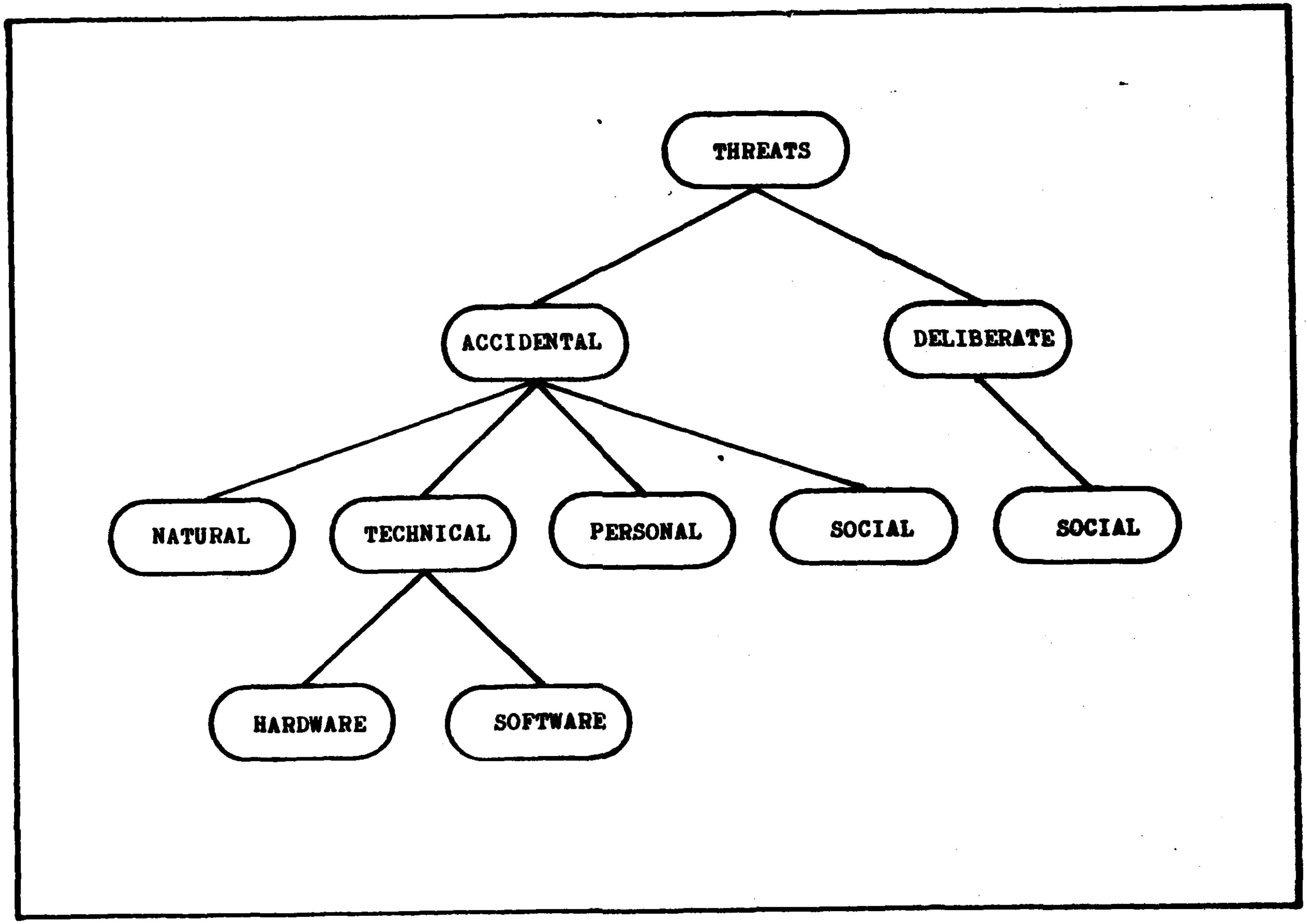


Figure 5.1 Decomposition of the Threat.

A. PHYSICAL THREATS

Physical threats come in a variety of forms that can be decomposed into two main areas - controllable and uncontrollable. Examples are:

CONTROLLABLE

- physical attack (civil disobedience, military assault, arson, locting, sabotage, vandalism)
- fire
- smoke, dust, and dirt intrusion
- bursting water pipes
- electromagnetic disturbance (lightening, vacuum cleaners, floor polishers)
- forcible entry and theft

UNCONTROLLABLE

- natural catastrophe (lighting, wind, tornado, earthquake, flood)
- aircraft crash
- bomb threat
- support non-availability

Controllable threats are those threats that can be prevented from occuring to a greater degree by the application of sufficient safeguards. Uncontrollable threats are those that cannot be prevented but whose effect can be minimized by proper procedures. The line between the two classifications is not well-defined as is evident by the presence of the same threat (lighting) under both categories. The line becomes clearer when specific computer installations are addressed along with the resources and the location of that installation. Note that the threat does not have to affect the computer facility directly. Just as an effective attack is the application of physical threats to the installation's support.

B. COMMUNICATION

The technical sophistication of communications facilities and devices is a growing trend in today's world. Man is able to communicate using satellite relay, laser technology, fiber optic mechanisms, and microwave transmissions. When these technologies are used in conjunction with computer systems, large amounts of data can be transferred over long distances at staggering rates. Conventional means of data transfer are also used. Telephone lines and direct line coaxial cable can be used in many cases. There are only three main types of threats that effect communications security but the implementation of these three differ significantly from one communications medium to the next thereby allowing for a great many permutations and combinations of threats. The main threats are:

- eavesdropping
- interception
- denial or destruction

Eavesdropping involves siphoning off information from a communication without detection. Interception is the interruption of a communication from its flow towards its intended destination and the redirection of that flow to an unintended destination. Denial/destruction is exactly what it says; the interuption of communications by such methods as jamming and destruction of communication equipment.

There is one other threat that can be logically listed here or under several other categories. This threat involves the browsing, interrogation, destruction, or alteration of information contained in a computer file through the use of external communication. This method works in reverse of the threats listed above. A recent example involved a ring of teenagers who owned personal computers and who were able to break in to the data banks of several large commercial institutions.

C. EMANATIONS

Emanations are the by-product of computing devices as they communicate with their peripherals (especially cathode ray tubes). The product of this communication is electromagnetic energy containing the the essence of the communication. This electromagnetic energy can be read by complicated but common devices. The range of most of these devices is restricted to a few hundred yards, at best, but the technique is very successful in the absence of specifically designed safeguards. Since this threat is relatively expensive for the penetrator to employ, the probability of this threat occurring is usually proportional to the sensitivity or classification of the information on file at the specific activity. The probability of an emanation threat to a local grocery store's inventory file, for example, is extremely remote.

D. HARDWARE

Hardware threats are those threats that normally affect the integrity of the computer or its stored data. The chief hardware threat involves the physical manner in which data is manipulated within the machine. The instruction set of a given machine is the set of commands that the machine is designed to understand. These instructions manipulate the machine's inner workings at various levels. If there is no provision as to the accessibility of these instructions among the various operations layers, an inadvertent or malicious penetration of all levels may occur. The potential effects are:

- the destruction/alteration of data
- the alteration of the operating system
- the absence of predictable manipulations

The unreliability of a computer manipulation is the chief threat to computer security. The changing of an instruction set or the absence of design features that ensure reliability is the threat's physical manifestation. Hardware security is more appropriately addressed in the next chapter (Countermeasures) because it addresses some of the ways reliability is aided.

E. SOFTWARE

Software threats come in two categories - lack of reliability and subversion. The reliability threat is as applicable to software as it is to hardware but the difference is that one is a physical concept and the other is a procedural concept. The software threat is more complicated than that of hardware because software is arranged in many layers (operating system, utilities, applications) whereas hardware is only one layer. This layering of software not only increases the area of vulnerability, it complicates the protection requirements.

Software subversion is another type of software threat that is much akin to software reliability but differs in that it is a deliberate rather than accidental threat. There are two main types of software subversion. One type is called a TROJAN HORSE. A trojan horse is a bit of code that is inserted into one of the levels of the software and is designed to provide an entry port for a penetrator. It can be summoned only through a pre-defined code that is designed so that the portal is not vulnerable to accidental discovery. It is an active threat , that is, it requires the penetrator to actively engage it. Another type of subversion is called the TRAP DOOR. A trap door is code that is inserted much like a trojan horse. The difference between the two is that a trap door requires no assistance from the penetrator other than its initial insertion. The program runs automatically when a target set of parameters is met. An example is the insertion of a trap door into an aplications package that processes classified data. The trap door activates itself through the use of the package and perhaps routes a second copy of a resulting classified report to a printer in another location. The penetrator could either pick up the report himself at the other location or he may allow the report to be delivered to him via the inter-office delivery system.

Software threats, although categorized into two general components, take on many disguises and are capable of causing losses in an infinite number of ways. The following chapter will deal with software threat countermeasures and may illuminate the topic appreciably.

F. PERSONNEL

Personnel threats in the computer environment are perhaps the bottom line in a study of computer security. All three categories of loss (availability, integrity, and confidentiality) are affected by the inadvertent or purposeful actions of humans. The form of the human threat can range from the simple absence of a key person at a computer facility to the covert activities of an undercover penetrator. The predominant personnel threat, of course, is the proclivity of the human to make errors.

A study conducted by Simonetti, Sass, and Monoky of the University of Toledo, [Ref. 10: p. 204] was designed to determine what changes had been made in computer security systems during the ten years prior to the study. The correlation between the number of changes made and the aspect of computer security that required changing due to inadequacy of previous safeguards was assumed to be high. The results of that study is presented in Table III above.

TABLE III

Changes Made in Security Systems

ORGANIZATION CHANGES MADE	PERCENT OF ORGANIZATIONS SURVEYED MAKING CHANGES
In human error control	100%
In physical access to computer	92%
In personnel screening	52%
In computer terminal access	52%
In warning systems for attempted false entry	31%
In new program testing	0%

The inference is that human interaction with the computer and its information is the threat most recognized by security system managers. The study cites another interesting statistic. Of all computer frauds committed and subsequently discovered, 58% were the work of ADP employees.

G. PROCEDURAL

Procedural threats are those that relate to the management function of control and affect the workflow process. Procedural threats are those that act upon those workflow points were control is passed from one function, element, or individual to another. Procedural threats can be accidental or malicious in nature and can be more accurately described in terms of safeguards designed to to counteract them.

VI. COUNTERMEASURES

Although the threats to the security of a computer system are numerous, there also exists an abundance of devices and procedures by which each can be countered. In order to intelligently employ an effective risk management program, the the manager must be aware of the countermeasure options he has available to him. The following paragraphs contain some of the considerations that must be made when choosing appropriate protection. Provided also is a listing of various methods used to combat specific threats.

A. PHYSICAL SECURITY

Physical countermeasures are employed to minimize the effects of dangers to the tangible assets of a computer system. Most of these methods use common sense and are directed at one specific aspect of physical security. The external and internal environment of a computer center are most important to physical security and depend upon some of the following considerations:

- physical location
- availability of fire and law enforcement services
- availability of medical facilities
- construction materials
- physical access routes

It is difficult to present a list of specific countermeasures without knowing the particular needs and operating constraints of a given system, however, it is possible to establish standards that guide the manager of computer assets. The following list of standards apply more or less to all facilities.

1. The structural soundness of buildings housing computer equipment should be adequate to: support the weight of computing machinery; accomodate electrical cabling and fire extinguishing systems; minimize the effects of wind, precipitation, and lightening; withstand, in some cases, the effects of explosions.
2. The employment of physical access controls to computer equipment, tape files, master documentation, master software copies, and environmental support (air conditioning, humidity control equipment, electrical power sources) should be established. (These steps are applicable to remote terminal locations as well.)

Some of the more common implementations of the above standards are:

- The number of windows and doors or other physical entry paths should be minimized consistent with local fire regulations.

- Chain link fences should be used where the classification of the information within dictates.

- The use of cipher locks, second access doors, holding areas, guards, and closed circuit TV can be employed where feasible.

- Exterior lighting should be employed where appropriate.

- Positve key control should always be maintained.

- Identification badges or other such devices are somtimes useful.

- Automatic fire warning, detection, and extinguishing systems with optional extinguisher delay to protect against inadvertant activation may be employed. Supplemental devices such as smoke removal systems, air filtration systems, and plastic sheeting used to cover equipment in the event of fire extinguisher activation are also useful.

- Uninteruptable power supplies, power surge insulators and appropriate power source switching devices can be installed.

- Air conditioning and humidity control devices are normally a necessity in large installations.

- Anti-static carpeting and controlled use of electromagnetic motors (floor buffers, vacuum cleaners) protect against the destruction of tape and disk files.

- Depending on the severity of the threat, those mechanisms considered critical to operations (air conditioning, humidity controls, fire detection and extinguishing systems) can be installed redundantly.

- The training of personnel is an important aspect of physical security. Fire drills, bomb threat drills, security compromise drills, and recovery drills should be conducted regularly.

B. PERSONNEL SECURITY

Personnel security is, perhaps, the most difficult aspect of an effective countermeasure program to maintain because it requires the greatest amount of subjective judgement from the manager. While no personnel program is one hundred percent effective, there are several basic steps that aide reliability and are commonly found in successful programs.

1. Screening

The complexity of a screening program depends, in large part, upon the composition of the population from which the selection is tc made and upon the potential losses that could result from incorrect selection. Whenever possible, a thorough screening of medical, employment history, scholastic, and psychiatric records should be accomplished and disqualifying criteria established. Personnel interviews and testing are also valuable tools during this phase of a surety program. In exceptional cases, a complete background investigations can be obtained.

2. Selection Criteria and Selection

Establishing selection criteria is probably the most subjective part of a personnel security program. If feasible, aide can be sought from professionals (psychiatrists, physicians, etc.) but the manager ultimately must make the final decision as to what criteria are to be used.

3. Maintenance

The selection of individuals for various positions begins the maintenance portion of the program. Maintenance programs include activities such as periodic training, briefing, and performance evaluations. Evaluation techniques abound but the most frequently used is day-to-day observation of an individuals habits, attitudes, physical appearance, and, if possible, after hours activities.

4. Debriefing

Debriefing is an aide that helps preserve a given security posture. The classical debriefing includes relieving the individual of classified and sensitive duties and material for a period prior to his departure and obtaining sworn statements from the individual. Debriefing in itself would not seem to be very effective, but as a part of a comprehensive program, it may be very useful.

The unpredictability of human behavior is perhaps the most complicated variable in any security program but a conscientiously pursued personnel program that includes the steps cited above can reduce personnel security risk appreciably and may localize the effects of personnel threats. A good personnel program is not the answer to total security. Systems that have many remote users often cannot apply personnel surety program techniques to the vast majority of their customers. In that sort of situation, other countermeasure types must be used.

C. COMMUNICATIONS SECURITY

Communications security, or the lack thereof, has influenced the outcomes of wars, the success of private companies, and the length of a head of state's term of office. Today, the technologies that enable man to convey information, especially digital information, complicate the security problem since not one of these technologies is completely secure.

Encryption is the most widespread method of countering communication threats. The technique uses some variable key to seed an encrypting algorithm. The algorithm scrambles the transmitted information into unintelligible code which can be unscrambled by a reversing algorithm at the information's destination. The same key must be used to seed the unscrambling algorithm. The keys can be changed periodically or they may change with each transmission. Historically, the usefulness of an encoding algorithm and its associated keys has been an inverse function of the time it remains in use.

One technique that deserves mention as an aide to communication security is not really an established security method at all, but rather, a side effect of a message routing schema. The method is called packet switching and it is used to solve complex message relay problems in medium to large networks. The stream of information is essentially chopped into variable length chunks called packets. Figure 6.1 illustrates the information that is affixed to the packet. The leading and trailing edge of each receive a coded sequence that essentially keeps each packet from combining with other packets. As the message leaves its source, a software generated header is inserted after the leading edge indicator. The header contains information such as the source of the message, the destination, the message number, the packet number, and other pertinent information. Each packet, with all its added information, is then routed to its destination via varying routes. As Figure 6.2 shows, all packets do not have to take the same path to the destination and may, in fact, arrive at the destination out of sequence. A hardware device at the destination then strips the added information from each packet and assembles the message in the proper order. The security aspect of packet switching lies in the fact that the various packets of a given message, may take different paths to the

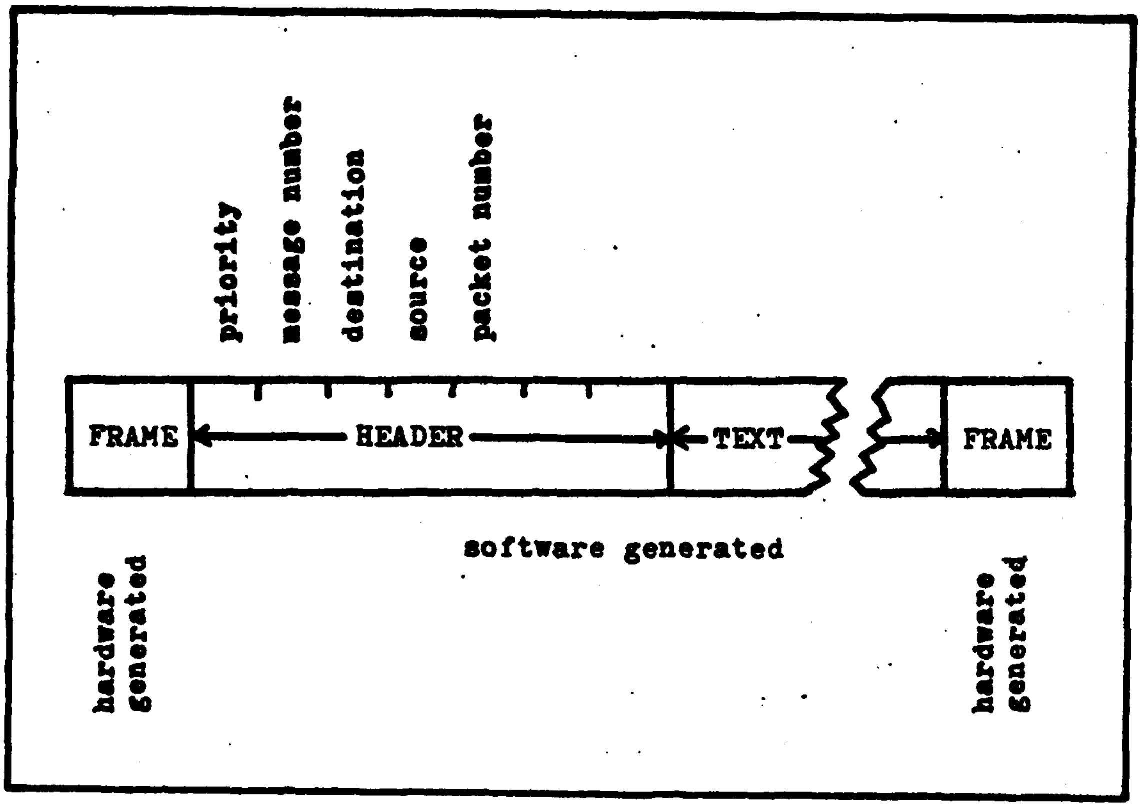


Figure 6.1 Typical Packet Constuction.

intended destination. A penetrator that has tapped one seqment of the network may or may not receive the entire message and may receive the packets out of sequence. Packet switching is not a reliable security method because the movement of the packets in the network is random and as such does not negate the possibility that an entire message may move over the same path.

Eavesdropping is the primary threat to communication security, but there are two other threats that account for a small percentage of the total communication threat. The denial of communication by jamming the communicating signal or by simply cutting the connecting cables is one of these threats. The only way that this problem can be averted is

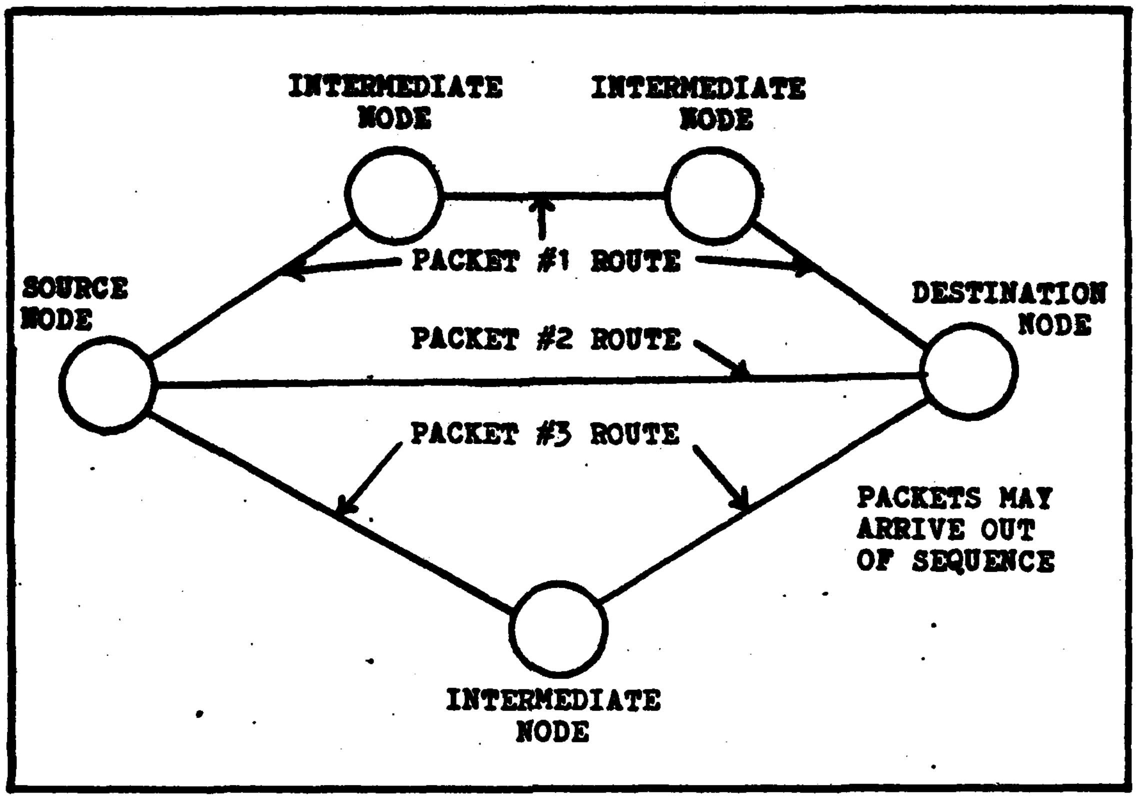


Figure 6.2 Representative Packet Switching Network.

through the use of back-up of transmission media. The other low-percentage threat is the re-routing of communications to unintended destinations. This is primarily a software problem and will dealt with later in this chapter.

D. EMANATIONS SECURITY

There are three basic countermeasures that can be used, individually or in parallel, to minimize information compromise through emanations interception.

1. The first method is simply the establishment of a physical buffer area around the computer installation. The radius of such an area depends on the strength of the emanations and the probable

sensitivity of an emanations receiving device, but a common figure used is 300 yards. The strength of the emanations signal is dependent upon the maintenance status of the equipment and the method of installation.

2. The second method is the reduction of the emanating signal through the use of appropriate sheilding. In many instances, computer complexes are lined with sheet metal.
3. The third method is the adjusting of the equipment to limit emanation strength.

E. HARDWARE SECURITY

Hardware countermeasures are designed to combat threats to data integrity. The physical implementations of hardware security devices take several forms but all are constructed to assure reliability in the internal procedures of the machine. The following hardware security features are common:

1. Most central processing units (CPU) utilize an instruction set that is split into privileged and non-privileged portions. Privileged instructions are those that are used by the operating system to perform its supervisory tasks and are not accessible to the user. Any attempt to invoke a privileged instruction from other than the operating system causes an exception condition and all processing of the job ceases. Unfortunately, many trapdoors use the interupt feature of the system as their activation signal. This type threat must be dealt with as a software threat as covered in the next section.
2. Memory locations within the physical machine contain various kinds of information. The operating system of

a computer is normally resident in some exclusive portion of memory and should not be accessible to the user. A typical method for eliminating 'potential attempts to alter the operating system or other critical storage area makes use of bounds registers. Bounds registers contain the addresses of the first and last locations of areas in memory that belong to individual data sets or programs. An attempt by a user program to access information outside the confines of the area defined by the bounds registers will cause an immediate exception.

3. Parity checking is another hardware convention that promotes data integrity. In simple terms, parity checking involves the inspection of an added bit that is tacked on to each data unit (byte, word, half-word). The added bit signifies whether the data unit contains an odd or even number of 1's or 0's. If the data is altered in some way, the chances that other adjacent data being altered is probable. As the data units are read, each of the parity bits are checked. If one of the parity checks do not match, a hardware exception will occur.

4. Automatic terminal identification is another hardware security measure. When a terminal is turned on, an automatic signal is generated that identifies that terminal. If the code received by the processor does not agree with the list of authorized terminal codes, the terminal in question is locked out. This situation can occur when a penetrator attempts to tap into a system using his own terminal.

The above methods of hardware security are generalized and cover a wide range of specific implementations. Other error detection, identification, and interrupt designs are frequently used and are usually automatic. The computer system manager should be interested in what methods are available on various machines so that intelligent judgements can be made during procurement evolutions. Beyond that aspect of hardware security, the manager has little control over hardware security.

F. SOFTWARE SECURITY

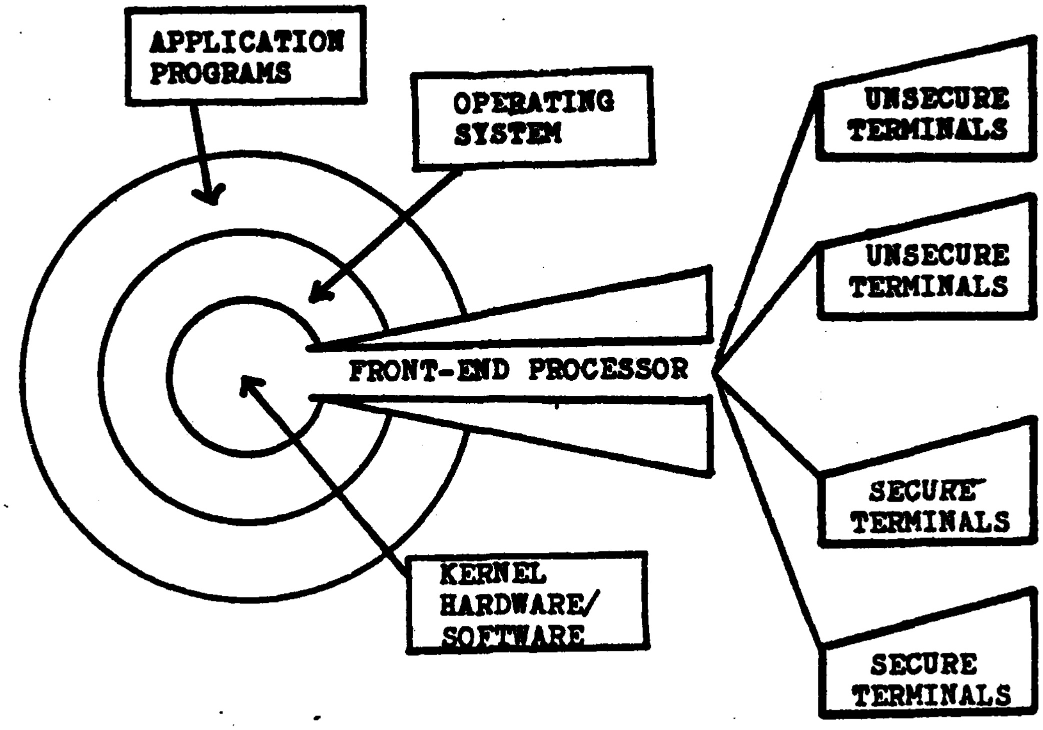
Software countermeasures are the most numerous type of security device and are normally designed to limit access in some manner. The following paragraphs describe some typical software security methods.

1. The Security Kernel

The security kernel is assentially a series of small subroutines that limits the access of other programs, including the operating system. The design of the kernel is based on a precise specification or matmatical model of its function. The model is composed of a set of access rules plus a set of user attributes (clearance, need to know) and information attributes (classification) [Ref. 14: p. 28]. Figure 6.3 shows the conceptual form of a security kernel. Note that it employs a front-end processor and that it is the base layer in the typical software hierarchy. The kernel programs objectively evaluate access requests (read, write, use) issued by a user, by another program, or by the operating system. The overhead of the kernel is reputed to be minimal.

2. Password Systems

Password systems are multi-layer software overlays (see Figure 6.4) that approve and deny access based on a user response to a password request from the system. User responses are matched against a password file. If a



[Ref. 14: p. 29]

Figure 6.3 Conceptual View of a Security Kernel.

correct response is made to a password request, access is granted; otherwise access is denied and terminal lockout may occur. Each user can either have multiple passwords that access different layers of information (programs, data, service requests), or have a single password that accesses all layers. Which ever method is used, the password file must also be protected in some way (encryption). Password systems are probably the most widely used of the software countermeasures, but, due to carelessness in the handling and assignment of the passwords, they are also the most widely penetrated.

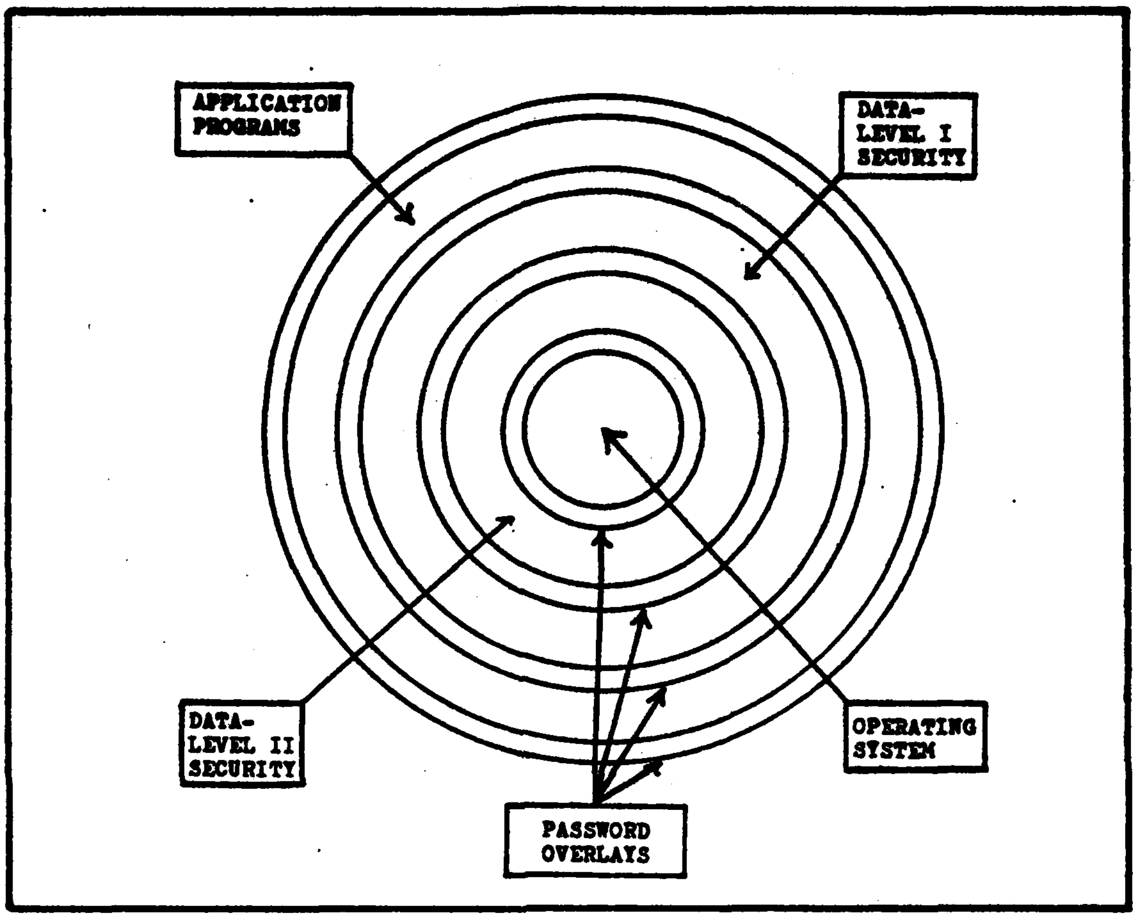


Figure 6.4 Layered Password System.

3. File Matrices

File matrices operate much like password systems. Each file is prefixed with a table that lists those programs and users that are authorized access. Instead of listing each user or using program, some matrices use classifications of users. Another variation may be constructed in either of the above ways and will contain additional information as to the level of use. The levels of use include categories such as "read", "write", or "use". "read" allows the user to read the file, "write" allows a user to write to a file, that is, modify it, and "use" allows neither "read" or "write" capability, but allows the use of the file. The matrices can be very simple or very complicated and depending on the the degree of complication, incurs a commensurate run-time overhead.

4. Program Auditors

Program auditors are programs designed to check other programs for integrity. A typical auditor will determine the number of lines of code in a particular program and compare its finding with a table containing the number of lines the program is supposed to have. This countermeasure is designed to prevent the insertion of trapdoors and trojan horses or the deletion of critical portions of a program. A much more complex version of the same idea is a program that checks the number of operators and the number of operands as well as the value of the constants in a program.

These are but a few of the software countermeasures employed by various installations. The security kernel is largely experimental at this writing (although the concept was originally identified around 1972) and the other methods have their individual failings and drawbacks such as excessive run-time overhead, the requirement for additional hardware, and the usage of an inordinate amount of storage space.

G. OTHER COUNTERMEASURES

The preceding sections have delineated several specific countermeasure methods that are designed to avert specific threats and threat classifications. Two very important countermeasures remain that are major parts of a risk management program.

The first of the two methods is auditing. Auditing entails the establishment of a comprehensive mechanism for confirming the reliability and the "correctness" of the system. The most important part of the auditing system is the construction of an audit trail. Audit trails are based upon single transactions and involve the establishment of corroborating evidence of who entered the system, what resources were used, and what the result was. It is beyound the scope of this thesis to attempt a full explaination of a audit trail model, however, the reader is encouraged to consult the writings of Bjork [Ref. 11: pp. 229-245] for a comprehensive disertation on the subject.

The second important risk management method concerns contingency planning. Contingency planning is the method by which recovery from the failure of countermeasures is accomplished. As such, it addresses every category of loss and every threat that a specific installation is vulnerable to. A typical contingency plan covers the topics listed in Table IV but peculiar needs of a particular ADP activity should also be included.

TABLE IV

Contingency Plan Tasks and Responsibilities

1. Identification of contingency conditions
2. Evacuation procedures
3. Powering down procedures
4. Flood and foul weather plan
5. Fire plan
6. First aid plan
7. Classified information securing/destruction planning
8. Back-up planning
9. Back-up support planning
10. Recovery planning
11. Temporary site requirements and selection
12. Hardware/software procurament planning
13. Emergency fund procurement
14. Contingency training
15. Mass medical emergency

VII. A COMPUTER SECURITY SURVEY

A. BACKGROUND

Chapters 1 through 6 have dealt with the scope of the security problem facing the computer systems manager, the legislation and directives concerning the topic, some risk management techniques, and the threats to computer security and the countermeasures frequently used to combat those threats. The purpose of the preceding chapters has been to give the apprentice computer systems manager a conversational knowledge of the topic and to emphasize the procedures, laws, and methods used by the manager in the performance of his duties. The managers of today's military computer installations must not only be proficient in their assigned tasks as managers, they must also be proficient as soldiers, sailors, airmen and Marines. As such the military computer systems manager must contend with physical fitness training for himself and his men, military training, drug and alcohol abuse programs, human rights seminars, gun polishing, boot shining, etc. It is therefore fair for a fledgling manager to inquire as to how one does it all. Further, in the context of this thesis, how is computer security treated in the typical military computer center and what priority is it accorded?

In an attempt to answer those questions, and to gain some first hand knowledge of the techniques employed by the military to combat computer fraud and misuse, a survey of a typical military data processing center was conducted. The survey approach was that of a learning evolution with the chief benefit going to the author. Since the remainder of this chapter takes on the characteristics of a critical review, the name of the computer installation surveyed will not be mentioned to preclude repercussions that might occur due to the content of the survey.

B. INSTALLATION DESCRIPTION

Computer installations are, for the most part, task organized. As such, the type and size of equipment, number of operators, communications media, and environment may vary widely. Since different installations require different security, a description of the surveyed computer center is presented to put the security critique that follows in perspective.

The Computer Data Processing Activity (CDPA) surveyed had recently completed a relocation to a new multi-purpose building that had been designed specifically for the unique environment that a computer center requires. The transfer of the organization's hardware was accomplished without major difficulty. The hardware presently operated by the CDPA consists of a 16 megabyte core memory, a CPU similar to an IBM 370, 46 disk units, 42 tape drives, and an external communications device. The operating system is similar to the IBM MVS/VM system and supports both a variety of local and remote job entry access devices. Figure 7.1 shows the organization of the local area network. The CDPA is one of seven major nodes on a world wide network with communication between nodes provided largely by commercial telephone and microwave media. Figure 7.2 shows the organization of the world wide network. As the figure shows, the network is organized so as to provide communication links between major nodes. Communication is accomplished, in most cases, via perferred routing but alternate routing is available in the event of degradation or failure of major node communication capability. The external communications device functions separately from the computer system thus allowing

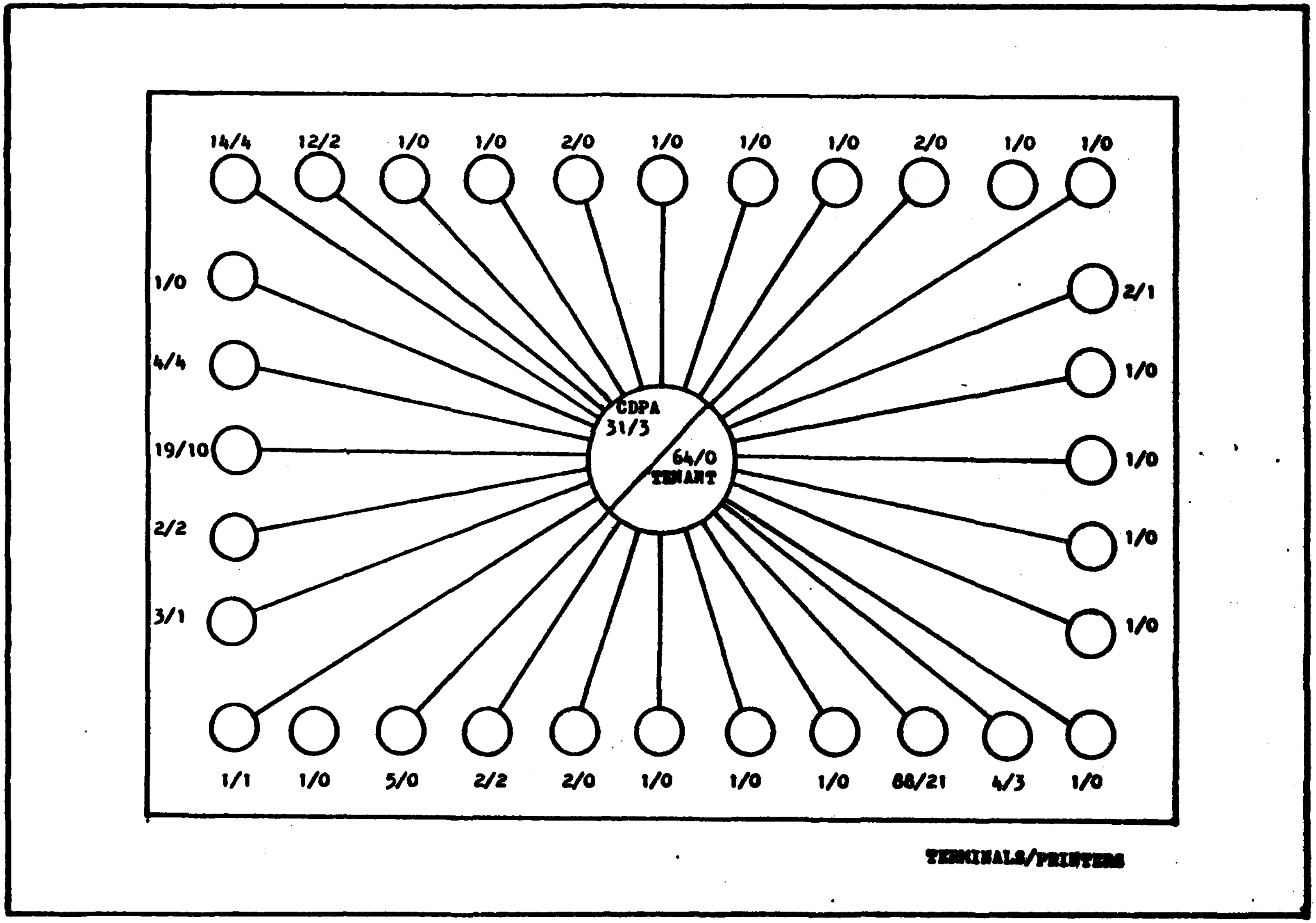


Figure 7.1 Local Area Network.

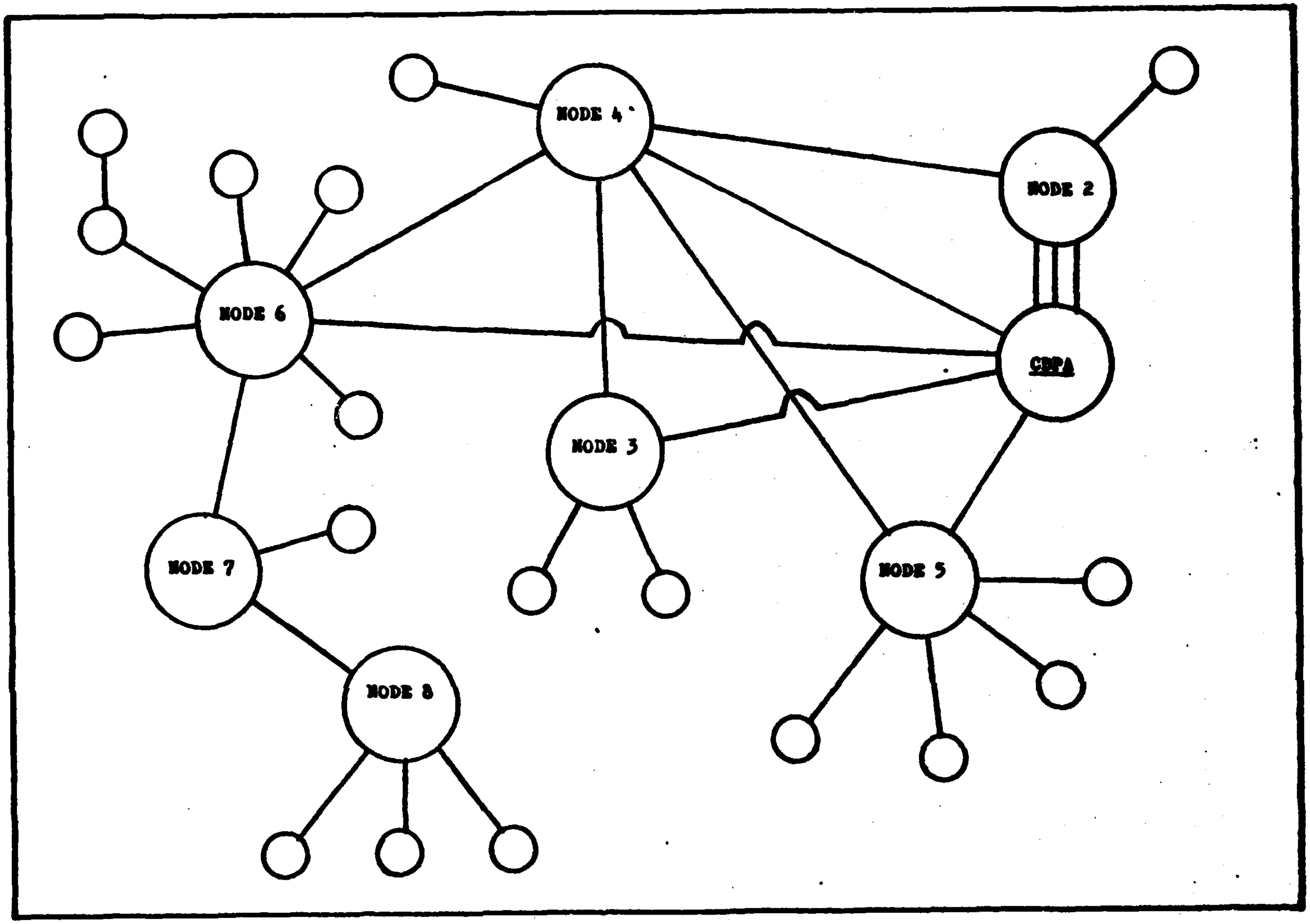


Figure 7.2 World Wide CDPA Network.

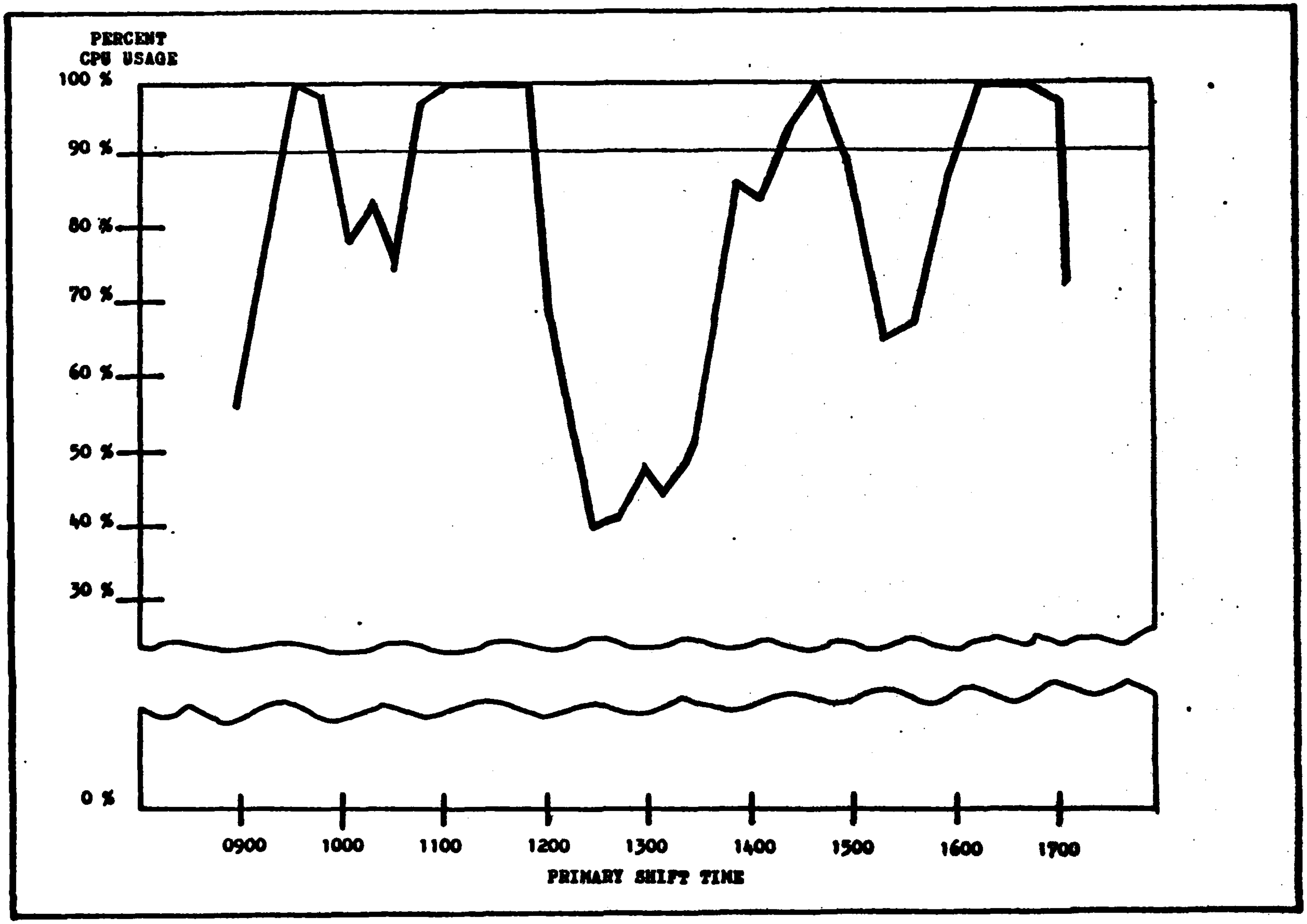


Figure 7.3 CPU Usage by Time of Day.

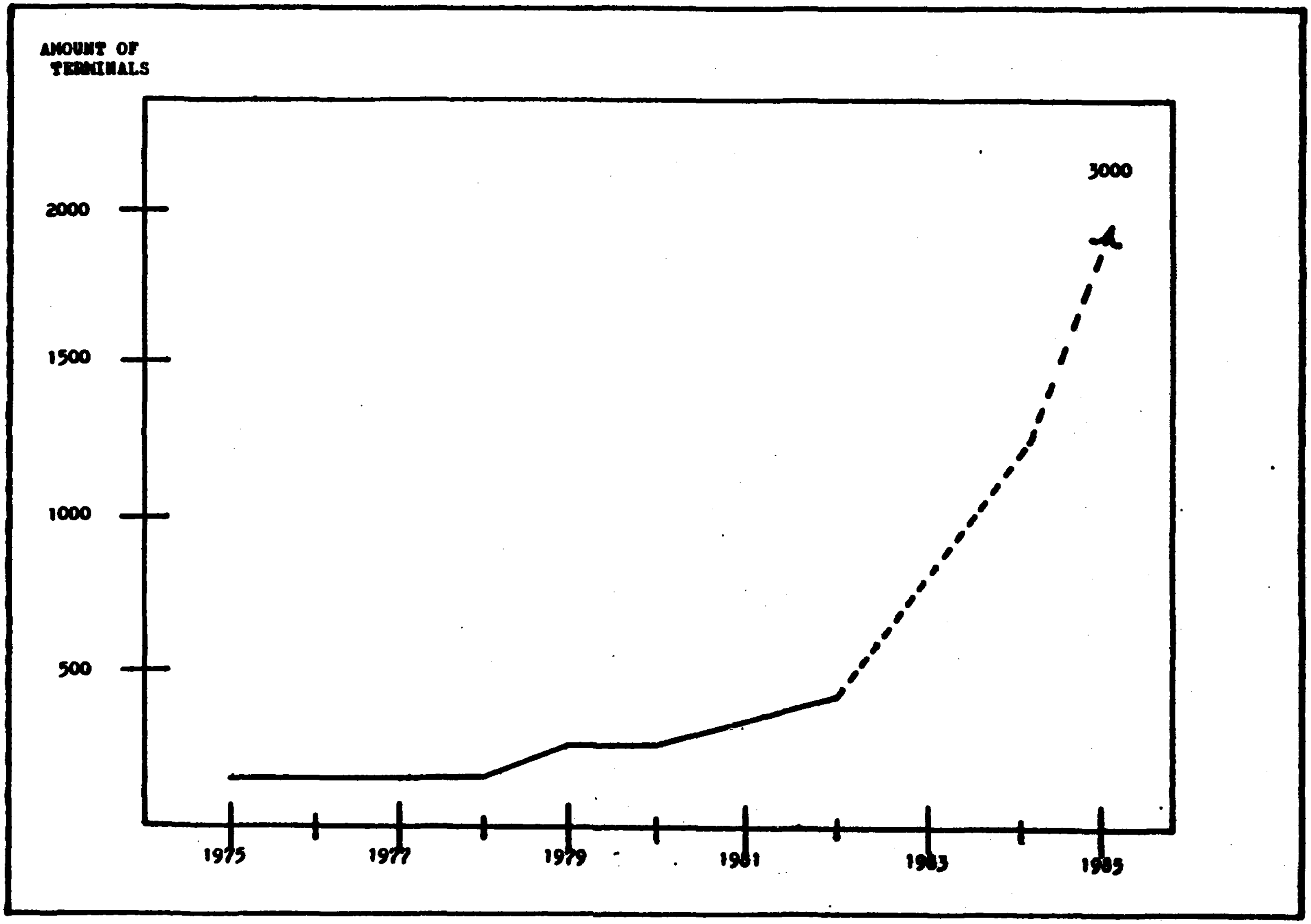


Figure 7.4 Interactive Terminals in World Wide Network.

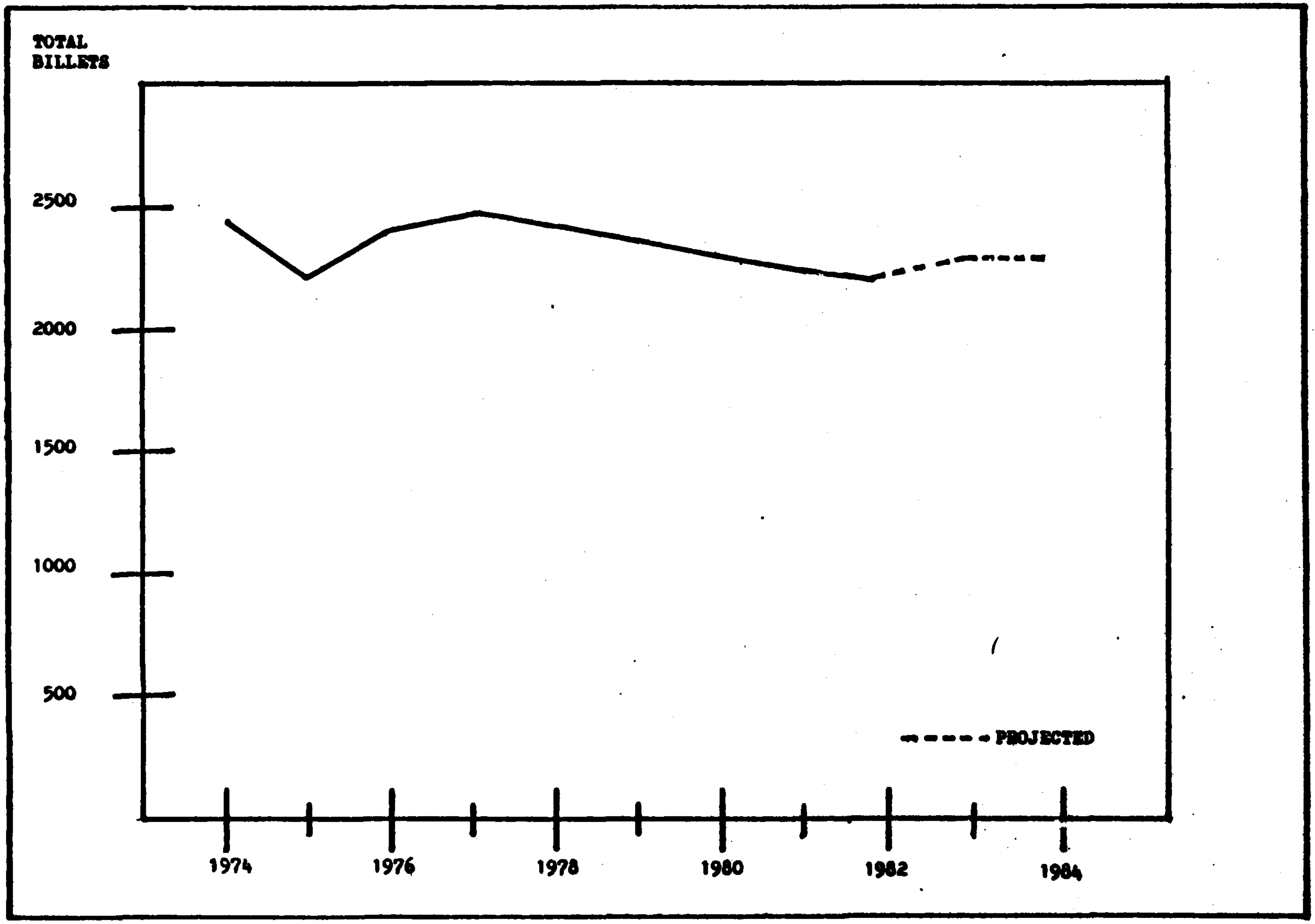


Figure 7.5 Data Processing Billets.

data transmission to occur during computer system down time. The local area network is supported by the same external communications equipment but there is no redundant routing feature employed.

The CDPA is manned by a military to civilian (GS) personnel ratio of 3 to 1. The director and his assistant are military and the several major departments are headed by an approximately equal number of military and civilian personnel. The CDPA, as well as the seven other major nodes support a variety of integrated databases and applications including personnel management, logistics, and operations support. The CDPA itself supports no classified processing but does process sensitive to moderately sensitive information. The security officer's position is assigned to the communications officer as a collateral duty.

The CDPA is currently experiencing a capacity problem as Figure 7.3 illustrates. The capacity problem is caused by inadequate CPU speed/capacity during peak interactive terminal demand and is causing a serious response time problem during those periods. Figure 7.4 shows the historical and projected growth of the number of interactive terminals in the world wide network. Assuming that the CDPA will support a fair share of the the anticipated growth, it is obvious that the capacity problem now being experienced will certairly be aggravated.

Another problem being experienced by the CDPA specifically and this particular military service in general, is the number of data processing billets available. Figure 7.4 implies that the personnel workload for the total system will soon increase rapidly. Figure 7.5 , however projects a rather stable number of data processing billets. It is expected that future hardware procurements will partially respond to this problem by way of technological advances. It is felt, however, that these advances will not accommodate the increased workload totally. The relavancy of this observation and that of the capacity problem to computer security will be established later in this chapter.

The attitude of top management toward the the security of their system is an important ingedient in the level of system security in any system. The weaknesses of this CDPA's security system, as identified in this thesis, came as no surprise to the installation's chief executives. Because of the absence of classified processing, the chief concern expressed in many of the interviews was for data integrity and protection. System confidentiality, it was observed, commanded very little attention.

C. CONDUCT OF THE SURVEY

The survey was conducted according to a consolidated checklist composed of inputs from two very comprehensive checklists [Ref. 7] and [Ref. 8]. Each checklist item was either personally observed by the suveyor or addressed in one of several interviews. For the puposes of this thesis, each major checklist category was reduced to comments about particular problems or highlights and/or a category posture statement. The main areas of investigation are listed below.

- Risk Management
- Physical Security
- COMSEC
- Emanations Security
- Hardware Security
- Software Security

- Personnel Security
- Contingency Planning

1. Risk Management

As discussed in an earlier chapter, risk management is the dynamic process by which the total of all system threats is assessed and through which the trade offs between security safeguards and the expenditure of resources are determined. The CDPA, it appears, has only a general skeleton of a risk management program in place. There are no local risk management publications and no one person is directly responsible for the preparation of a risk management program. Risk management, at best, is in an infancy stage within the CDPA. In the author's opinion, a valuable opportunity for the initiation of a risk management program was foregone during the conception and planning stages of the the CDPA's recent relocation. An obvious flaw in the design of the new building, in terms of computer security, was discovered during the survey and addressed under physical security later in this chapter. If the building had been designed with security in mind from the outset, (for instance, with a risk management team as part of the design committee), the physical security would have been enhanced.

Although no formal risk management system exists at the CDPA, it was obvious to the observer that the level of security awareness was extremely high. In small systems, a very high level of security awareness may be substituted successfully for a risk management program. In an organization the size of the CDPA, a risk management program is highly desireable. The complexity of the CDPA system is such that a highly organized and systematic approach to the security, integrity, and confidentiality of the system assets is essential.

2. Physical Security

With the exception of some obvious, easily correctable discrepancies, the physical security of the CDPA appears to be superior. The building in which the CDPA resides serves both the CDPA and a closely related activity. Both organizations maintain independent operations and very little infrigement on each other's spaces is required. The building itself is constructed of fire retardent materials. It is located on a military reservation with regular and frequent military police patrols. Response time of both the military police and the fire department has been been tested at less than two minutes. The building's fire alarm, detection, and extinguisher systems, the electrical power system, and the environmental system are all redundantly installed. Storage areas and user access points are physically separated from the main computer room.

There are two chinks in the physical security system. Two very large windows are located in the computer room. Although the windows are reputed to be very strong and highly resistant to breakage, their presence causes excessive solar heating during the warmer months of the year. The windows are located directly over a large bank of disk drives at one end of the room and over the communications device at the other. The increased heat has not caused an undue number of disk drive failures or communications problems to date, but the service life of both devices may be adversely affected if positive measures are not taken. There is currently a work order on file at the local facilities maintenance organization requesting that the windows be removed and replaced with concrete and brick. The request had been outstanding for several months at the time this survey was taken.

The second physical security problem is the absence of a suitable archival storage area. At present, archival file storage is located in the basement of the building in a cinderblock vault. The vault has its own environmental control and fire extinguishing systems, but it is located next to a supply stcreroom filled with materials such as continuous form paper and duplicating fluid. In the author's estimation, this arrangement is not adequate for archival storage and is inconsistant with the CDPA's concern for data integrity. A possible remedy for this inadequacy might be the use of an underground vault located outside the perimeter of the building. Not only does this arrangement minimize the threat of fire from the adjacent storeroom, it protects the archival files from building collapse in case of fire or natural disaster.

3. Communications Security (COMSEC)

The CDPA does not employ any extraordinary COMSEC techniques or devices. Data communication between the CDPA, its remote job entry sites, and other nodes in the world wide network is accomplished over commercial telephone lines and microwave relay. Packet switching and encryption techniques are not used because of the absence of classified data files resident on the CDPA's storage media. Further, the users of the information, superior levels in the command chain, do not support encryption because they percieve no need or utility from the technique.

There is at least one reason to support the employment of COMSEC measures. Although no single piece of information is, in itself, classified, a particular processing application could combine information in such a way that the aggragated information could, in fact be useful to a potential penetrator. There is little doubt that the computer professionals of the CDPA have recognized this

possible loophole but their hands are politically tied. Their task is not procedural at this point, it is political. The resistance of seniors in the command chain to the incorporation of COMSEC must be overcome before someone else locates this weakness in the system.

4. **Emanations Security**

The CDPA has no emanations security procedures or devices in place. The multiprogramming feature of the operating system is, in the opinion of the installation commander, a sufficient confidentiality safeguard against the intentional procurement of sensitive information through emanations interception. Note also that the cost of shielding a facility the size of the CDPA against emanations threats would most likely be prohibitive.

5. **Hardware Security**

The equipment operated by the CDPA is modern and incorporates many of the hardware features conducive to data protection into the system. The following is a listing of the hardware security attributes present in the CDPA equipment.

- Privileged and non-privileged instruction set
- Register error detection and redundancy checks
- Error detection during fetch cycle
- Memory bounds checking
- Automatic program interrupts
- Remote input/output identification
- User isolation
- Controlled supervisory mode access

6. Software Security

At the beginning of this chapter, it was noted that the CDPA was experiencing a CPU capacity problem. Boehm [Ref. 12: p. 13] points out that the cost of software begins to increase increase steeply at approximately the 85% saturation of CPU or memory capacity of a given system. Although he does not explain the sources of his observation, the general explaination for the sudden jump in software cost is a drop in programmer productivity caused by an emphasis being placed on software efficiency. Wulf [Ref. 13: p. 95], observes that

> more computing sins are committed in the name of efficiency (without necessarily achieveing it) than for any other single reason...

Efficient code, albeit desireable, has the innate quality of being difficult to read and understand. This certainly complicates the task of the maintenance programmer. Add this complication to the fact that the CDPA anticipates programmer workload to increase and the stage is set for the emphasis to be removed from proven software design methods. The end result of an emphsis on efficient running code is that security takes a backseat and the unstructured code becomes a effective hiding place for subversion techniques. It is unlikely that the CDPA will have much success with security software until their capacity problems are solved. It must be acknowledged, at this point, that the CDPA has plans to acquire additional CPU capacity. In addition, a software overlay - essentially a password system - is being tested for use on the major nodes on the world wide network. At the time of this writing, however, the only data protection software in place was a data base language system using an integral data dictionary.

7. Personnel Security

Personnel security at the CDPA appears to be adequate. The screening of personnel for duty in the data processing field in this branch of the military is complete and very selective. Most of the personnel at the CDPA have "SECRET" security clearances and each person is required to attend intensive security training prior to assuming duties. Regularly scheduled refresher training is accomplished in accordance with the local security plan. Due to the difficulty encountered in the retension of highly trained personnel, there is no mechanism for rotating personnel through various billets. This problem is service wide and not directly attributable to CDPA management techniques.

8. Disaster Contingency Planning

Prior to the relocation of the CDPA, a comprehensive contingency plan was developed by the CDPA director and his staff. At the time of development, the CDPA was located in an older building considerably more vulnerable to physical threats and natural disaster. The plan included purchasing contingent capacity from a computer services vender. The plan was rejected by upper level management because it was too expensive. There exists some mutual backup capability between the major nodes in the world wide network and the feeling is that priority processing could be begin within 48 hours of a disaster using other nodes' capability, but there is no published contingency plan and the recovery plan is, of course, dependent on the availability of archival files. The fine points of this informal recovery plan are obscure both to the observer and, it is suspected, to CDPA personnel. The topic of backup is mentioned at every meeting of CDPA commanders but the formal declaration of a plan is probably years away.

VIII. CONCLUSIONS

The intended purpose of this thesis is to present the reader with an overview of computer security and to encourage further study of the subject by those who categorize themseleves as computer systems managers. The major underlying objectives of this work are to convey the broad scope of the topic, cite the importance of risk management, and to present what the author believes to be the overall status accorded computer secuity in the contemporary ADP environment. This last objective is the subject of the following paragraphs.

While it is difficult to generalize about a population using a sample size of *one*, the implications of the survey summarized in Chapter 7 have been informally corroborated by conversations with active and past computer professionals. The most pointed commentary is a article by Air Force Colonel Roger Schell, [Ref. 14: p. 16-33], past instructor at the Naval Postgraduate School in Monterey, California and currently the Deputy Director of DOD Computer Security Evaluation at Ft. Meade, Maryland. In the article, Colonel Schell warns of the dangers that result from a lack of an aggressive security posture and is critical of the present state of military computer security. In view of this observation by the foremost computer security expert in the Department of Defense, the following observations are made.

First and foremost an information system should perform its intended task as well as its conceptual planning allows. A secondary, but important portion of the information system's task is to ensure that the quality of the information it contains is preseved and that the disemination of that information is made selectively. Saying that another way - the information system should ensure availability, integrity, and confidentiality of the information it stores and operates upon. If an information system does not provide these assurances in some greater degree, it is probable that one of the following conditions are present:

- management ignorance
- lack of resources
- lack of security maintenance

The first condition is not widespread at the installation level. It is more a failing of management levels above where managers are not likely to be computer-oriented personnel and, as such, have very little, if any, feel for the vulnerability of computers. Unfortunately, those same upper-level managers also control the financial and personnel assets required to implement security assurance.

The second condition is a problem faced by both military and civilian managers and is self-explainatory.

The third condition, as Schell points out, is the continuing reliance on established security measures without periodic review. He cites historical references of misplaced trust in security measures (the breaking of the German and Japanese communication codes during World War II) and urges managerial personnel to continually evaluate security measures.

The priority accorded computer security in today's ADP community appears to be low. Since the tools and the technology for effective security are available, one must deduce then, that complacency is the chief cause for this undesireable status. It is therefore incumbent upon the computer systems manager to promote risk analysis and to educate at all levels of management on the effects of a poor security program. Until progress is made in reducing the complacency level, the very fabric of the decision making process - information - will remain unreliable.

LIST OF REFERENCES

1. Allen, Brandt, "The Biggest Computer Frauds: Lessons for CPA's", *The Journal of Accountancy*, v. 39, May 1977.

2. Pritchard, J.A., *Computer Security: Risk Management in Action*, NCC Publications, 1978.

3. Federal Information Processing Stanlards 41, *Computer Security Guidelines for Implementing the Privacy Act of 1974*, 30 May 1975.

4. Moffett,Jonathan, "Zen and the Art of Computer Security, *Information Privacy*, v. 3, May 1981.

5. Federal Information Processing Standards 31, *Guidelines for Automatic Data Processing Physical Security and Risk Management*, June 1974.

6. Carullo, Michael J., Shelton, Fred A., "Quantitative Evaluation: A New Way to Measure Computer Security", *CA magazine*, v. 113, October 1980.

7. U.S. Marine Corps UNCLASS, MCO P5510.14, PCN 102 084902 00, *Marine Corps Automatic Data Processing (ADP) Security Manual*, 2 January 1981.

8. Diebald Research Program 184m54, *Security Measures and Disaster Contingency Plans*, undated.

9. United States Navy UNCLASS OPNAVINST 5239.1A, *U.S. Navy Automatic Data Processing Security Manual*, 15 August 1978.

10. Simonetti, Jack L.; Sass, C.Joseph; Monoky, John; *A Statistical Analysis of Computer Fraud and Computer Security Systems*, presented at the Annual Meeting of American Institute for Decision Sciences, 11th, New Orleans, La., November 19-20, 1979.

11. Bjork, L.A., "Generalized Audit Trail Requirements And Concepts fo Data Base Applications", *IBM Systems Journal*, v. 14, No. 3, 1975.

12. "Software and Its Impact: A Quantitative Assessment", *Datamation*, v. 7, May 1973.

13. Wulf, W.A., *A Case Against the GOTO*, paper presented at the proceedings of Association of Computing Machinery Conference, October 1972.

14. Schell, Roger R., "Computer Security: The Achilles Heel of the Electronic Air Force?", *Air University Review*, v. 18, January-February 1979.

BIBLIOGRAPHY

Burke, E. L., Computer Security Technology: The Second Generation, paper presented at the proceedings of the Spring Computer Conference 79, San Francisco, California, 26 February - 1 March 1979.

Comer, M., "Computer Fraud: It takes A Thief", Business Matters, V. 2, December, 1980.

Fisk, A.J., The Security Officers' View of Security, paper presented at the Carnahan Conference on Countermeasures, University of Kentucky, Lexington, April 6 - 8, 1977.

Honeywell Information Systems, Inc., Computer Data Security, 1982.

Hussain, D. and Hussain, K.M., Information Processing for Management, Richard D. Irwin, Inc., 1981.

Landwehr, C.E., "Formal Models for Computer Security", Computing Surveys, v. 13, September, 1981.

Larson, D.L., Computer Data Security, M.S. Thesis, Naval Postgraduate School, 1974.

Lupton, W.L., A Study of Computer Based Data Security Techniques, M.S. Thesis, Naval Postgraduate School, 1973.

Myers, P.A., Subversion: The Neglected Aspect of Computer Security, M.S. Thesis, Naval Postgraduate School, 1980.

Norman, A.R.D., "Computer Fraud: The Villian's View of the Opportunities", Electronics and Power, v. 24, 1978.

Parks, E. J., The Design of a Secure File Storage System, M.S. Thesis, Naval Postgraduate School, 1979.

INITIAL DISTRIBUTION LIST

		No. Copies
1.	Defense Technical Information Center Cameron Station Alexandria, Virginia 22314	2
2.	Library, Code 0142 Naval Postgraduate School Monterey, California 93940	2
3.	Department Chairman, Code 54Js Department of Administrative Sciences Naval Postgraduate School Monterey, California 93940	1
4.	Commanding Officer Marine Corps Central Design and Processing Activity Quantico, Virginia 22134	1
5.	Curricular Officer, Code 37 Computer Technology Systems Naval Postgraduate School Monterey, California 93940	1
6.	Marine Corps Representative, Code 0309 Naval Postgraduate School Monterey, California 93940	1
7.	Professor Norman Lyons, Code 54Lb Naval Postgraduate School Monterey, California 93940	1
8.	LCDR William Shockley, Code 52Sp Naval Postgraduate School Monterey, California 93940	1
9.	LT. S.K. Crowder 3704 Lakota Road Alexandria, Virginia 22303	1
10.	Major William D. Helling 2511 Windsor Avenue Dubuque, Iowa 52001	3